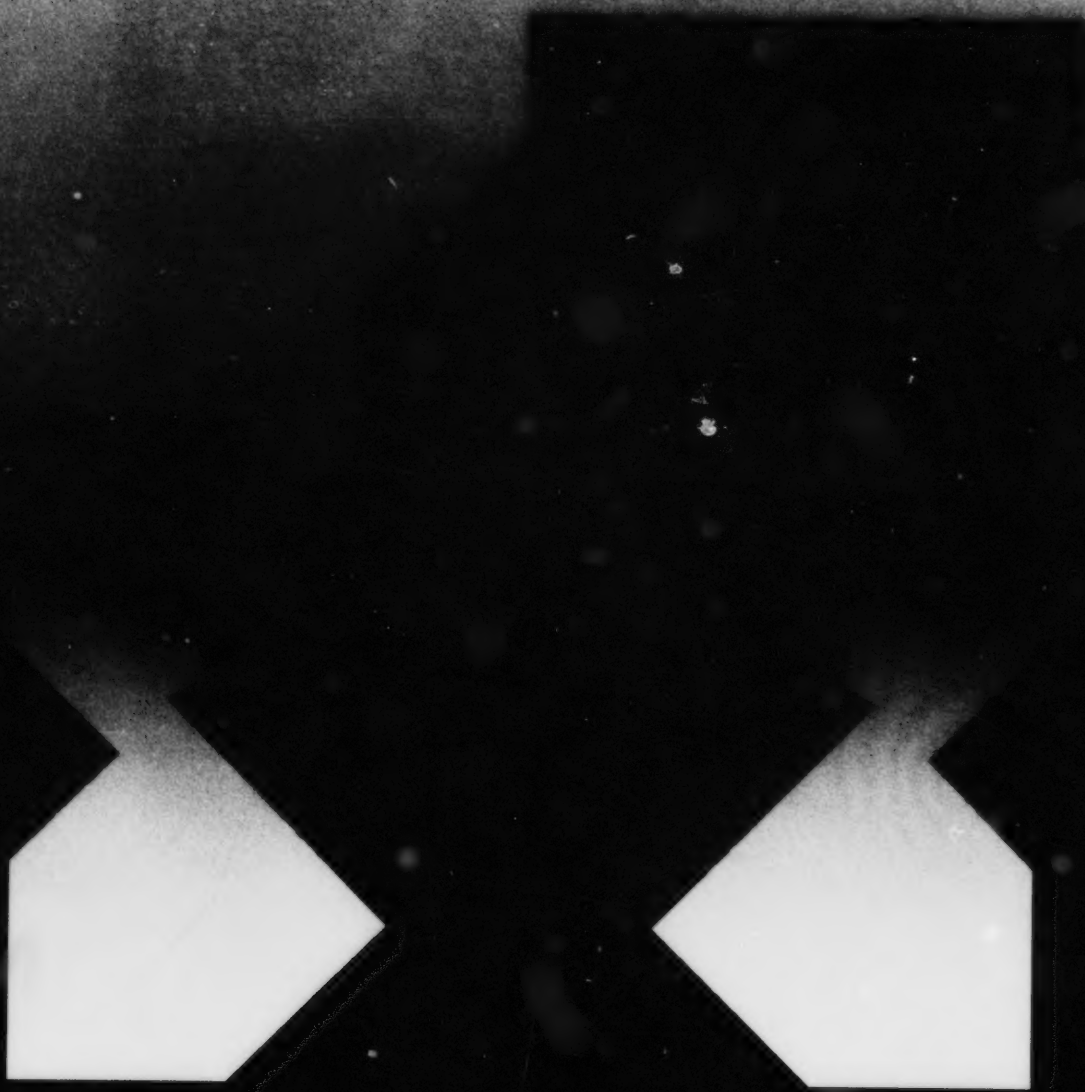


Canada Mortgage
and Housing
Corporation



Société canadienne
d'hypothèques et
de logement



CMHC Helping to
house Canadians

RESIDENTIAL INTRUSION ALARMS

Residential Intrusion Alarms

Canada Mortgage and Housing Corporation

Residential Intrusion Alarms

A Report Prepared for the
Canada Mortgage and Housing Corporation

by Jaroslav Zenchuk

Ottawa August 1988

Jaroslav Zenchuk is an Ottawa-based freelance researcher and writer.



ACKNOWLEDGEMENTS

I would like to thank the following people for giving generously of their time to provide me with information for this report:

James P. Harris

Honeywell-Amplitrol, Ottawa

Jim Turnbull

MSP Centre, Rexdale, Ontario

Donald Parnell

ABC/Ademco Distribution, Ottawa

Marilyn Little

Ottawa Cableguard Inc.

Dave Duggan

Federal Alarms, Toronto

Gil Toppin, Paul Hallam, E. Cestra

Underwriters' Laboratories of Canada

Frank Henderson, John Maplesden

Canadian Alarm and Security Association

Peter Wilson

Capital Region Alarm Association

Stephen Marshall

Nepean Police Force

Lew Penny

Royal Canadian Mounted Police

Terry Sullivan

Hamilton-Wentworth Police Force

I would also like to thank Phil Dupuis of the Consumers' Association of Canada
and Margaret Maine of the Ottawa Public Library.

CONTENTS

1. Introduction	6
Background	6
Scope of the Work	7
A Note on Product Performance	9
2. Responsible Alarm Ownership	12
Question #1: Do I Really Need One?	12
The Choice is Yours	14
Neighbours	15
False Alarms	16
3. Theory and Design of Intrusion Alarms	20
Wired or Wireless?	23
Recent Developments in Wireless Alarms	27
4. Sensors	33
Perimeter Sensors	35
Interior Sensors	45
5. Controls	66
Panels	66
Remote Controls	75
6. Reporting Systems	78
Local or Remote?	78
Central Station Alarms	83
7. The Cost of Protection	87

8. Choosing an Alarm Company	91
How to Recognize a Security Professional	95
Glossary	98

[1] INTRODUCTION

Background

The alarm industry is large and growing rapidly. One source estimates the value of security products sold in the U.S. in 1986 at \$5 billion, \$250 million of which is spent on residential security. There are perhaps a dozen Canadian companies engaged in producing systems, components or supplies for the alarm industry (the exact figure depends on which companies are considered to be Canadian, and the type of activity considered to be manufacturing), several hundred in the U.S. Some are large corporations, others consist of one or two people working in a small office.

At present, there is no restriction on the type of equipment that can be manufactured and/or sold in Canada. There are no universally recognized standards for residential alarm systems,¹ and no testing, certification or licensing of residential systems or of companies selling residential alarm services is required. Testing by the Underwriters' Laboratories of Canada

¹ The Underwriters' Laboratories of Canada has prepared standards that govern the construction, installation, performance and monitoring of commercial and mercantile alarm systems and equipment, but even in these cases ULC certification is not mandatory. ULC has also prepared a Preliminary Standard for Household Burglar Alarm System Units (1974) and a Guide for the Installation and Classification of Residential Burglar Alarm Systems (1986). Again, compliance with either the guide or the standard is strictly voluntary--with one exception. Smoke and fire alarms, which fall under the Hazardous Products Act, must be ULC approved. A residential burglar alarm that is used to power and annunciate a smoke or fire detector, being part of the fire or smoke detection system, would also require ULC approval. Installation of non-approved equipment in such instances is an indictable offense.

(ULC)--the sole Canadian agency engaged in such work--is on a voluntary basis: firms submit their products for ULC approval in the hope of getting a market edge. Electronic components can be imported and assembled by anyone with sufficient know-how, identified with a make or model number, and placed on the market. Although most manufacturing has been, and continues to be, in the hands of responsible firms whose reputation rests on the quality of their products, the field remains a complex and treacherous one for the average consumer. Faced with competing claims from scores of alarm companies, and lacking reliable up-to-date information about available alternatives, the buyer is frequently at the mercy of salespeople whose overriding motive is profit.² This project was commissioned by the Canada Mortgage and Housing Corporation as a first step toward providing homeowners interested in purchasing an alarm system with reliable, up-to-date information about the industry and the wide range of options available to them.

Scope of the Work

The study has two parts. The first part is a written report on the theory and practice of electronic burglary protection, including a description of the equipment available and how it works. The discussion, which is strictly generic (no manufacturers or product models are mentioned by name), pays

² Fortunately, changes are afoot. The industry is becoming increasingly aware of the need for regulation and standardization. Efforts are under way to coordinate nation-wide licensing of dealers and to establish performance standards that will be recognized throughout the industry. The Canadian Alarm and Security Association (CANASA) has presented the provincial Solicitors General with proposals for self-regulation of the industry, and is negotiating with the ULC for joint development of national performance standards.

particular attention to the strengths and limitations of each type of device, noting the conditions under which its use is appropriate and the environmental factors that can affect performance. The report offers practical ideas about choosing a suitable system and a reliable alarm company. It pulls together information that may form the basis of a CMHC advisory document aimed at enabling homeowners to make an informed choice about electronic intrusion alarms.

The second part of the study is a catalogue of equipment used in residential alarm systems (for CMHC use only, submitted under separate covers). The problem of identifying what equipment is available to homeowners is a complex one. Most products are designed for commercial and industrial applications, but in many areas the distinction between commercial and residential equipment is becoming increasingly blurred. Manufacturers are adopting a modular approach, if only to reduce inventories. Commercial panels can be converted to residential use--and vice versa--by adding or removing "modules," or circuit boards. For example, zone expanders can be added to a residential panel to increase the number of protection zones from 10, say, to 30, making the panel suitable for use in a store or warehouse.

The problem is compounded by the fact that some alarm companies contract with manufacturers for the production of "customized" products, which are made to the firm's own specifications and sold under its name. But for their labels, these products may be virtually identical to those sold by a competitor. Only an examination of their circuitry could determine whether they were the same or substantially different products.

For these reasons, the survey of equipment included in this study relies primarily on information supplied by leading national distributors, rather

than retailers. In Canada there are about a half dozen major distributors. Among them, they handle products manufactured by some thirty or forty Canadian, American, European and Far East firms. According to one estimate, the equipment distributed by these six firms represents 95% of the professionally installed equipment available in Canada.³

In addition to professionally installed equipment there is a large and thriving do-it-yourself market. Do-it-yourself kits are sold by department stores, hardware stores, consumer electronics outlets, locksmiths and retailers of building supplies. The contents of these packages change rapidly and without notice. As well, there are countless mail order houses that advertise in consumer magazines and sell their wares directly to consumers on either side of the border.

The catalogue of equipment makes no attempt to be comprehensive. Instead, it presents a cross-section of devices now on the market. It focuses primarily on equipment currently sold in Canada, but some devices that are so far available only in the U.S. have also been included.

A Note on Product Performance

Apart from noting areas of possible weakness (typical causes of false alarms

³ This estimate may be high: certain American manufacturers do not distribute their products through the distributor network, preferring to sell exclusive rights to market their product to regional franchisers. Individual retailers are also free to import and sell products manufactured in the U.S. or other countries--all that's needed is initiative and a tolerance for the paperwork involved. These products do not appear on distributors' inventories and only a thorough survey of the retail market--something well beyond this study's scope--would turn them up.

in certain sensors, for example), the report does not include specific performance data. For one thing, information about product performance is virtually nonexistent. Product evaluations conducted by consumer protection agencies are often invalid when only a year or two old as products disappear from the market or are altered as new technologies become available. ULC data is not available to the public without prior written permission of the manufacturer. Much of the new equipment is never tested because it is not submitted to the ULC by the manufacturer. Even if it were, new equipment is produced at such a rate that it is doubtful if the ULC could keep up with the demand.

Because of the rate of change in the industry, it is unlikely that performance data, even if it were available, would be especially useful to the average buyer. The report therefore focusses on describing how electronic detection systems work and what buyers should look for in a particular piece of equipment: solidity of construction, protection from moisture and temperature changes, freedom from radio-frequency interference and line transients, sensitivity and range adjustments, and so on. With this kind of information, a buyer can make a wise choice not only among the options available today, but among those that will become available in one or two years.

Further, it is fair to say that most equipment sold--at least that which is sold by professional alarm companies--does what it is supposed to do: it detects change, whether it be a change in temperature, weight, or location. The detecting ability of burglar alarms is not really the problem. The problem is one of discrimination--the ability to discriminate between authorized and unauthorized entry, between normal environmental disturbances

and those caused by an intruder--and this is a much trickier problem than simple detection. Manufacturers have devised various technological solutions to the problem of discrimination, and some of these are outlined in this report. But in the absence of actual test data, it remains for the individual buyer to decide which of the solutions are likely to be effective.

Given the present lack of regulation and standardization in the industry, buyers should proceed with caution, keeping in mind that, when it comes to alarms, by and large you get what you pay for.

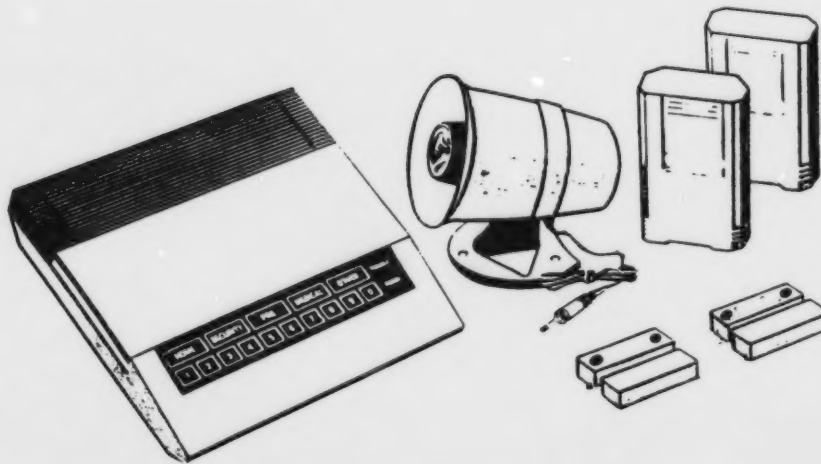


Fig. 1. Do-it-yourself wireless alarm kit.

[2] RESPONSIBLE ALARM OWNERSHIP

Question #1: Do I Really Need One?

A carefully selected and properly installed burglar alarm can be a worthwhile investment in security. But not everybody needs one. A burglar alarm might be a good choice for people who:

- . live in a remote location or where normal surveillance by neighbours is impossible;
- . own an expensive home filled with valuable possessions;
- . spend prolonged periods away from home on business trips or at the cottage;
- . because of their high social visibility, reputation or the nature of their work run a higher than average risk of becoming victims of burglary or other crime;
- . live alone and are willing to pay for the peace-of-mind that an alarm system can provide.

On the other hand, if you live in an average neighbourhood where your home is much like those around it, have well-secured doors and windows and take basic security precautions, chances are you don't need one.

The second question to ask is "Why do I want one?" The answer could have a bearing on the type of system you choose. If you are chiefly concerned with the personal safety of your family, you will want a system that will not only scare off an intruder but will also summon help quickly and reliably. By asking this question in advance you may find that an alarm system is not the answer to your problem. One homeowner installed an alarm system in an effort

to dissuade prank-playing youngsters. The youths quickly learned how to deliberately trip the system, providing themselves with a new amusement at the homeowner's expense. The frustrated owner eventually disconnected the system.

There is evidence that burglar alarms reduce the likelihood of an intrusion.¹ But the security and peace of mind they provide come at a price. To the cost of the equipment, its installation and (if you so choose) its ongoing monitoring must be added the annoyance of false alarms, the added complication that alarm ownership and use will impose on your life, and the limitations it will place on your freedom of movement. Before investing in a system you should ask not only whether you need and can afford one, but also whether you can tolerate one.

¹ Some insurance companies recognize the deterrent value of an alarm system by offering reduced premiums on homeowners' policies (typically 5-10%). Generally speaking, only installations that use ULC-approved equipment and are monitored by a ULC-approved monitoring station qualify for a reduction.

The Choice Is Yours

Most burglaries are crimes of opportunity committed by non-professionals. The majority of these crimes could have been prevented had the homeowner taken basic security precautions and exercised common sense. Even the best alarm system in the world will not protect you if your home's doors and windows are weak, the locks are ineffectual, or if you don't use them. Readers should consult CMHC's publication on home security (Protecting Your Home Against Burglary) for the basic security measures that every homeowner can and should take before installing an alarm.²

Correctly installed and used, an electronic burglar alarm system will do exactly what it is supposed to do--discourage most burglars. It will not guarantee that your home will not be burglarized. There is no such thing as perfect security. Responsible alarm ownership means realistically assessing your security needs and choosing a system that matches those needs, your lifestyle and the design and layout of your home.

As a responsible alarm owner it is up to you to choose a system that will do the job properly and with a minimum of inconvenience to yourself, your neighbours and the authorities. That means buying quality components. In an effort to cut costs and increase profit margins, some manufacturers will use inexpensive parts which wear out quickly or are easily damaged. Many inexpensive models begin to deteriorate a few months after they are installed, causing frequent false alarms. They become a nuisance to the public and the police and a waste of money to their owner who, in all likelihood, will eventually discard them.

² Many police forces will help homeowners determine their security needs.

Neighbours

If you install an alarm, you should make every attempt to involve your neighbours. This is true whether you have an alarm that sounds locally (local alarm) or one that reports to a monitoring station (central station alarm). With remote reporting, a local alarm acts as a backup communication in the event that the remote system is out of order or has been incapacitated by the intruder. If you are using only a local alarm, the cooperation of your neighbours is doubly important, as they are your nearest source of help.

Planning ahead is essential. Consider carefully who will respond to the alarm and how. If you are at home, you might choose to investigate the disturbance yourself. If so, you risk confronting the intruder, creating a potentially very dangerous situation. The best policy might be to call the police from the safety of your bedroom.

If you will be away, do not assume that your clanging bell or wailing siren will be investigated. Most people are so used to hearing sirens and horns that they will ignore them, assume that something is already being done or just pass by because "it's none of their business." Here are some good pointers to follow for alarm owners:

- . Inform your neighbours that you have installed an alarm and demonstrate what it sounds like;
- . Obtain their cooperation in phoning your home if they hear the alarm to verify that the emergency is real (be sure they have your correct address and phone number). If there is no answer, or if the answer they receive suggests that something may be amiss, they should call the police. You can devise a simple password that would indicate an all-clear; if a caller

receives a response that does not include the password, he or she should call the police. Under no circumstance should a neighbour take it upon himself to investigate the intrusion. Remember, too, that it is better that the police receive three or four calls than none at all because everybody assumed that someone else had made the call. With a little organization, a designated caller can be identified to avoid multiple calls to your home or the authorities.

- . Give your most trustworthy neighbour, friend or relative a key to your home. This person, who is designated as the authorized respondent, should accompany the police on their investigation, be instructed in how to turn off and/or reset the alarm (if it does not automatically do so), and take charge of your home until you return. This person may also be instructed in how to handle other alarm emergencies (medical, fire, etc.)

False Alarms

Every false alarm diminishes a system's credibility. Neighbours soon become indifferent and even police and private security agencies can become less than enthusiastic in their response. Plagued with a series of nerve-jangling false alarms, homeowners can grow lax about using their systems: they may turn the system on sporadically or not at all. In the end, false alarms can defeat a security system as effectively as the most skilled burglar.

Any system is only as good as its weakest link. Unfortunately, the weak link in many alarm systems is the homeowner. According to one source (CANASA), 70% of false alarms are caused by user error.³ People forget to

³ Other sources put the figure as high as 90%.

close doors and windows before turning on the system, or if they close the door, they forget to lock it, and the alarm is tripped when the door is opened by wind or a delivery person. People often leave the home and arm the system correctly, but then rush back, having remembered something they had forgotten, and trip the alarm when they re-enter the home. Pets, children and visitors unfamiliar with the system are also common causes of false alarms.

Good security practices are essential. If you install an alarm system, you should learn how to use it properly and teach all family members how to do so as well. You may be required to make some changes in your personal habits and lifestyle. If you are unwilling to make such adjustments you should reconsider the idea of installing an alarm.

The remaining 10 to 30 percent of false alarms are caused by defective equipment, improper use (use of equipment in an application for which it was not intended), faulty installation or poor adjustment. Most of the problems in this category are caused by powered interior sensors.

Each type of sensor (sensors are discussed in detail in Chapters 3 and 4) has its own areas of vulnerability. Some can be triggered by a passing truck, household pets, the draft from a hot air register or fan, or by rapid changes in temperature or humidity. Others can be set off by an interruption in the power supply, a ringing doorbell or phone, or the neighbour's fire or burglar alarm. Some sensors are affected by power surges (as when a heavy appliance is turned on or power is restored after an outage, or when lightning strikes) and by various types of radio-frequency interference.

Some false alarms have little to do with the quality of the equipment. Seasonal changes, for example, can have an effect. Doors and windows can expand and contract with temperature, become warped from repeated wetting and

drying or become misaligned in their frames as the home settles. Any of these factors can change the tolerance between contacts, causing a false alarm. Wind can rattle a loose door or window enough to set off an alarm. Wires can be pinched during installation or when other work (such as renovation) is done.

Many of the causes of false alarms are predictable and can be eliminated or reduced by using quality equipment and having it properly installed. Others are virtually unpredictable. One dealer tells of the house tabby that caused no problems until it grew past a certain size and, thanks to its added weight, began tripping a pressure-sensitive mat. Occasionally, false alarms are caused by several factors acting in unison or by small changes in user routine--changes that, in the absence of an alarm system, would have been taken for granted.

Finally, a very few false alarms (or perhaps more than most dealers would like to admit) are caused for no apparent reason whatsoever. Industry insiders have a name for these mysterious and annoying phenomena--they call them "swingers."

The question is not whether false alarms will happen but what you, the alarm owner, will do about them. Responsible alarm ownership means taking each false alarm seriously, finding the cause and, if possible, eliminating it. You may have to adjust the system, your personal habits, or both.

In some areas the incidence of false alarms approaches 98%. A few municipalities, including Calgary, Montreal and Nepean, have enacted bylaws aimed at stemming the tide of false alarms, and several others have legislation pending. In Calgary, alarm owners must obtain a permit which can be revoked if the system causes three or more false alarms in a calendar year.

Fines may be levied against repeat offenders. A number of police forces will temporarily suspend services to homes with a history of false alarms.

[3] THEORY AND DESIGN OF INTRUSION ALARMS

Every alarm system has three parts:

- . the sensors
- . the controls
- . the reporting system.

Sensors are devices that detect an intruder and send a message to the control panel. The panel is the brains of the system: it analyzes the messages it receives from the sensors and decides what to do about them. Some messages it will ignore (those received from a temporarily by-passed sensor, for example); others it will relay to the homeowner via a set of LEDs (light emitting diodes) or a liquid crystal display (a few of the newest systems use a voice synthesizer). These messages may tell the owner that a battery needs to be replaced, that a door has been left ajar, or that a sensor has malfunctioned. If the panel decides that a signal sent by a sensor constitutes an intrusion, it will activate the reporting system--a local bell or siren, or a digital communicator that alerts the monitoring station.

Most modern systems consist of separate components. There is a good security reason for this: a component system is much more difficult to defeat. Vulnerable components (such as the master control panel) can be hidden from view while the sensors themselves can be located in strategic places to detect an intrusion. Some alarms consist of a sensor with a built in control and noisemaker. The problem is that the sound of the siren will betray the location of the control, allowing a burglar to locate and destroy both. This is also the failing of the many inexpensive portable, battery-operated door or

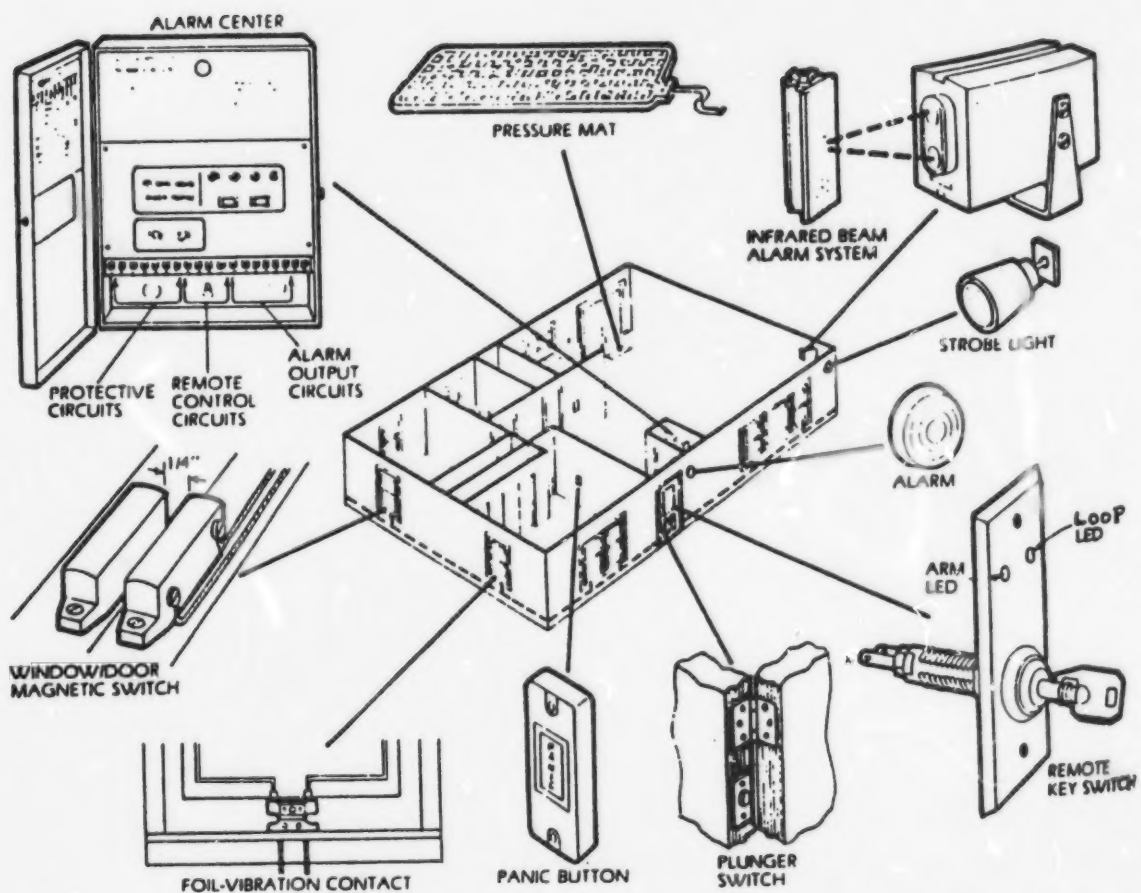


Fig. 1a. Components of a typical alarm system.

window alarms designed for use on a single entry point: destroying the sensor ends the alarm.¹ In a component system, destroying the sensor will not silence the alarm: the remote noisemaker continues to sound, drawing its power from the hidden panel.

A component system permits greater flexibility. It can be more carefully tailored to a particular environment, providing increased coverage and greater resistance to false alarms. Components also afford greater ease of operation. By locating remote controls in key locations throughout the home, the system can be armed, disarmed or configured to suit a family's activities during various parts of the day.

Modern systems provide layers of protection. The first layer consists of the perimeter sensors, which guard the main points of entry into the home: its doors and windows.² The perimeter system is backed up with a network of interior sensors designed to detect any intruder who manages to bypass the perimeter system.

Why not provide perimeter protection alone? First, because it is generally impractical to protect every possible opening to the house. Determined

¹ These devices, usually referred to as point-of-entry alarms or portable alarms, are battery-operated. They are either self-contained capacitance devices or consist of a single magnetic contact or spring-loaded switch with piezo-electric buzzer attached or built in. Some have a sensitivity adjustment, others do not. Most are imported from the Far East.

Most police (and probably most burglars) regard these devices with disdain. On the other hand, a consumer protection agency that tested several of these products in 1981 found them "uncomplicated and predictable," although a few were overly sensitive and prone to false alarms (most of the models tested are no longer available). Better models may provide added security to travellers in motel and hotel rooms; the cheaper units are little better than toys. In either case, they are seldom used for home security and are not dealt with extensively in this report.

² It may be argued that the first line of defense consists of the decals which, affixed to the windows and doors, warn that the home is equipped with an alarm system. The vast majority of burglars requires no other deterrent.

intruders will gain access through upper-story windows, skylights, air-conditioner openings---even some vents. Some, assured of a large payoff and certain escape, may cut through a garage wall, a floor or roof. A perimeter system may keep a burglar who has gained access to a home through unconventional means from using its main doors to carry off some of the owner's bulkier possessions. As well, it may not be possible (or affordable) to install some perimeter sensors fully concealed from view, in which case they may be detected and foiled by a particularly determined and resourceful intruder (there are no fool-proof sensors). A good perimeter system provides a first line of defense and will discourage most burglars. Interior traps are used as a second line of defense against the persistent few who are less easily dissuaded.

Why not use interior traps alone? Because the interior sensors will alert you only after the intruder has broken in. In fact, unless you have a sensor in every room and hallway, an intruder may spend considerable time in your home before actually setting off an alarm. The idea is to keep intruders out in the first place. A perimeter alarm acts like an early warning system that detects an intruder while he or she is still outside your home. Most modern alarm systems use a combination of perimeter and interior sensors.

Careful consideration should be given to the type and location of sensors. Every sensor has its strengths and weaknesses; some work better in certain environments than in others. Their location will be determined by the type of sensor used, the home's layout, the presence of environmental factors that could trigger false alarms, and the habits and lifestyle of the residents. This is where knowledgeable alarm professionals will earn their keep. The best installers can tailor a system to a given home's unique parameters,

choosing the most effective sensors for the job and mounting them in the most strategic locations. With a little planning and ingenuity, a single sensor can be used to do the job of several (a pressure-sensitive mat installed under a hallway carpet, for example, can effectively trap that area as well as a pair of ultrasonic sensors located at either end of the hall--and for a fraction of the price). Components can be mounted so that they protect each other; any attempt to approach and disable one sensor will be detected and reported to the control by another. Proper location of sensors can also mean substantial savings due to easier installation.³

Wired or Wireless?

One of the first questions that will confront the homeowner who has decided to install an alarm system is this: Should he/she choose a wired or wireless one? In a wired system, all sensors are connected to the control panel via a continuous copper path, along which the alarm signal is transmitted when a sensor is tripped. Power must also be delivered to sensors via the system's wiring. Wireless systems use compact battery-powered radio transmitters to send a radio-frequency alarm signal from the sensor to the panel by way of a

³ An experienced security professional will also know countless ingenious ways of getting an intruder to reveal his/her presence. This is the guessing-game world of selective trapping, decoys and baiting. An expensive camera might be placed in plain view, for example, as a lure. What the burglar doesn't know is that the camera is holding down the plunger of a hidden switch. Another ploy is to bug the door of the liquor cabinet or bathroom. There are endless such possibilities. Some are useful, some excessive, others downright inappropriate. It will be up to the homeowner to decide.

strategically located receiver.⁴

Professional security companies have long been leery of wireless systems, leaving this market to the do-it-yourselfer. They regarded wireless alarms as interesting novelties, but not worth considering when it came to serious security. Despite their higher installation costs, wired systems were often less expensive to install (perhaps because wireless alarms required greater design sophistication and additional equipment, ie., transmitters and receiver). Wireless systems were also considered to be less reliable and subject to signal jamming and interference. As well, a wireless system could not be tested for correct operation, as a wired system could, at the press of a button. Batteries could run down (and frequently did, each at a different time) and components could malfunction without the owner knowing, often remaining in that condition for weeks or months before being discovered. Transmitters were often large and bulky and had a limited range.

There are indications that this situation has changed. Miniaturization and mass production of electronics, together with the rising cost of skilled and semi-skilled labour, has made it possible for high-quality wireless systems to be manufactured and installed at competitive prices. Reliability and immunity to radio frequency interference have been improved. The use of integrated circuits, which consume virtually no current, has significantly extended battery life--up to 5 to 8 years, according to one manufacturer. Transmitters are now much smaller and less obtrusive (some are about the size of a credit card, though thicker; others can be fitted into the body of a rather bulky

⁴ It should be noted that some "wireless" systems are only partly so, since the sensors must still be wired to transmitters and the receiver must be wired to the panel. Wiring may also be required for an external siren. In other designs, the receiver and transmitter are combined in a control "console" and sensors may have built-in miniature transmitters.

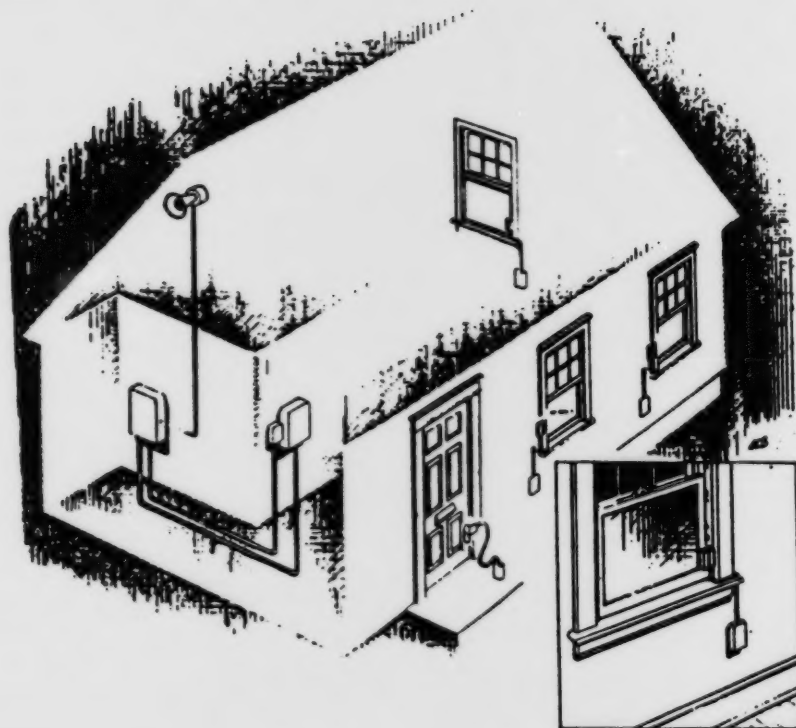


Fig. 2. Wireless alarm system. Note transmitters attached to sensors on doors and windows.

magnetic contact). Some people in the industry now believe that wireless alarms are the way of the future.

Even the earliest wireless systems had the advantage of portability. This is an important consideration, given that security systems may cost several thousand dollars and that Canadians tend to move on average once every 4.5 years.⁵ Wireless systems are also more easily reconfigured after a home is remodelled or its furnishings are rearranged.

Ease of installation is another important advantage of wireless designs. Whereas installation of a wired system can occupy a team of installers for several days, a comparable wireless system can sometimes be installed by a single technician in a matter of hours. Wireless installations also have a minimum effect on the structure--a great selling point with most homeowners.⁶ In a wired system, all sensors must be wired to the control panel. This involves running wires inside walls (not an easy task in the case of walls filled with insulation), through floors and ceilings, bricks and blocks, under baseboards and carpeting, into basements and attics. Ideally, all wiring and most perimeter sensors in a wired system should be concealed from view, both for security and aesthetic reasons, and many hours of labour and much energy may be expended in the pursuit of this goal. Achieving a neat and efficient

⁵ It can be argued that the components of a wired system, less the wiring of course, are equally portable.

⁶ A few firms, in an effort to avoid retrofit problems and keep down costs, are negotiating with builders to pre-wire new homes and apartments during the initial construction. Wiring layouts are generally designed in consultation with the alarm company. Although the plan is ostensibly a good one, there are risks involved. For one thing, there is no guarantee that the subsequent homeowner will purchase an alarm system from the company that did the wiring. Also, some installations have been plagued by problems caused by wiring that was damaged during later phases of construction. Finally, despite the best of intentions, pre-wired systems often turn out to be significantly more expensive.

installation requires considerable planning, skill and ingenuity (superhuman patience can be a definite asset). And for all installers, time is money. Posed with a difficult installation problem, installers may cut corners. The result may be a pinched wire or faulty splice that will continue to plague the system for weeks or months to come. Not surprisingly, the cost of a wired system is often more a reflection of labour costs than of the price of hardware.

There are other problems: wires become dislodged, worn or damaged during maintenance or renovation work. Splices work loose and soldered connections can deteriorate.⁷ To their credit, however, properly installed wired systems do provide a high degree of security and reliability. Better systems will be virtually invisible and very difficult to detect or disable. One indication of their effectiveness is that virtually all high-risk commercial alarm installations (jewelers, furriers, etc.) are wired. The vast majority of residential systems now being installed are also wired.

Recent Developments in Wireless Alarms

Most wireless systems use radio waves to transmit the alarm signal to the receiver.⁸ Because of this, early wireless systems were plagued by radio

⁷ A few firms avoid problems caused by bad splices and shorts by "home-running" all wires back to the panel, without the use of junction boxes.

⁸ Although most wireless systems use radio-frequency communication, other mediums are also available. These include infrared, ultrasonic and line-carrier systems. Each medium has its disadvantages: infrared is limited to line-of-sight transmission; ultrasonic waves are blocked by walls and doors; and line carrier systems, which use existing house wiring to transmit an alarm signal from the sensors to the panel, will not work when the power is off. I could find only one system that uses any of these technologies--a perimeter system based on sound discrimination that uses line carrier

frequency interference from neighbouring systems, CB radios, garage door openers, and so on. In the middle 1970s, a digital transmission technique was developed that allowed the signals to be coded. The technology made automatic garage door openers more reliable by eliminating the tendency of adjacent units to trigger one another. It also opened the door to more reliable wireless alarms. During installation, a wireless system can be programmed with a unique "house code," which allows the panel's microprocessor to distinguish signals originating from within the protected premises from those that may come from outside. Each sensor may also be given a unique code that identifies it to the panel and allows it to report to the panel regarding its condition and status.

This is the area of system supervision. It is true that many low-cost wireless systems are still unsupervised--that is, the sensors communicate with the receiver only when an alarm condition exists. Faults and dead batteries can go undetected unless a manual inspection is carried out. In most top-of-the-line modern wireless systems, however, some kind of supervisory capability is built in. Thanks to microelectronics and improved software, each transmitter-equipped sensor can be programmed to report to the panel once a minute, hourly, daily, or according to any other predetermined schedule (the trade-off is that the more frequent the test signal, the quicker the batteries wear down). In this way a sensor can report whether it is currently active, whether it has been tripped or not, whether it is functioning properly, and

transmission.

the condition of its batteries.⁹ The control's microprocessor analyzes the coded message and displays the information to the homeowner using built-in LEDs or other visual/auditory display. In a central station alarm, the control may also inform the monitoring station. If a sensor fails to report on schedule, the fact is noted at the panel, and the system may go into alarm.

The development of highly sensitive, crystal-controlled ("superheterodyne") receivers gives modern wireless systems an impressive range (300 metres is not uncommon) and selectivity, reducing--but not eliminating--the chance of interference from other sources. Interference is further reduced in some systems that are designed to transmit in the FM band (most wireless transmitters operate in the AM band), taking advantage of FM's increased ability to lock in on a signal.

Use of multiple-channel receivers and coded signals allows wireless systems to be subdivided into different zones and functions, similar to wired systems. Perimeter and interior sensors, as well as fire, panic and medical alarms, can all report on a different channel.¹⁰ This makes it possible to turn off part of a system (to open a window for ventilation, say) while the rest of the system continues to function normally. It also allows an open door or window to be easily located and shut before the system is turned on. In older

⁹ In some systems, the supervision works in the other direction, with the control panel periodically "polling" each sensor, checking on its health, status and battery condition.

¹⁰ In a hardwired system, zones are created by wiring groups of sensors together on the same protective "loop," or circuit. To avoid unwieldy masses of wiring at the panel, some models use a branching system. A series of "transponders" is connected to a single pair of trunk wires that runs throughout the premises, and one or more sensors is connected to each transponder. The system provides two-way supervision between the control and the various transponders, reporting on status and condition. If each transponder supports only a single sensor, the network becomes a point-by-point annunciation system (called "Point-ID").

systems, if a door was left ajar, the system would either not arm, or it would arm and sound a false alarm. Zoning or point-ID capability is also an invaluable aid in troubleshooting faults.

For all their sophistication, modern wireless systems are not without their problems. A signal may be reflected (by mirrors, metallic wallpaper, foil-backed insulation etc.), causing the separate parts to arrive at the receiver at different times and from different directions. If the signal parts are out of phase, they may cancel one another, creating a "null" or dead spot. State-of-the-art systems incorporate various high-tech solutions to the problem, with varying degrees of success. In more basic systems the problem can sometimes be solved by relocating the receiver or transmitters (sometimes a few inches either way will do the trick). Occasionally, signals may be blocked or attenuated by building materials, such as metal framing or studding in walls (sometimes found in highrises). Some systems that function reliably in a bungalow or apartment behave erratically in a multi-level home, where the signal must travel between floors. Wireless systems sometimes cannot be used in older frame homes that have wire mesh installed behind the plaster walls.

Exceptional care must be exercised when installing a wireless system. Considerable time can be spent in adjusting and relocating components for best signal reception. In order to extend battery life, some sensors are designed to send a single signal and then wait for two or three minutes before they can be tripped again. This makes walk-testing time-consuming--time that adds to the total cost of the system. In a few cases, it may not be possible to use a wireless system at all. If in doubt, installers can pretest the home to see whether a wireless system will work. In all cases, signal strength at the receiver should be tested after the installation is complete.

Another--although infrequent--problem with wireless systems is signal clash ("contention"), which results when two or more signals arrive at the receiver simultaneously. Some receivers can be overwhelmed by multiple signals and ignore both.¹¹ Some systems solve the problem by designating a different time slot in which each sensor will report to the transmitter. Others rely on multiple signals, short signal length and random transmissions to avoid the problem. Most of the newer receivers are programmed to give priority to certain signals, typically in this order: fire, panic, burglary, medical alert, tamper, fault, status and low battery.

Some systems (particularly less-expensive models) still suffer from radio frequency interference (RFI). Nearby appliances operating on alternating current (air conditioners, for example), portable phones, police and ham radios and even computers can generate enough RFI to keep a sensor's signal from reaching the control panel. A recent development, used on many current high-quality panels and sensors, is SMD (Surface Mounted Devices) technology. Circuit elements are mounted directly onto the circuit board; the absence of leads prevents the induction of voltage from any stray radio-frequency signals.

Many modern systems now use both wired and wireless components. These hybrid designs consist of a basic wired system, with wireless sensors and transmitters used to protect outlying areas (outbuildings, for example¹²) and places that would be too difficult or expensive to wire in a conventional manner (as in the case of solid masonry construction or in buildings with

¹¹ Hardwired systems, which look for any break in the circuit, have an advantage here.

¹² This may not work if the main house has aluminum siding.

cement floors).

How to choose? Here are some points a homeowner might consider:

- . How difficult will it be to install a wired system and to conceal the wires in your home? If you live in an apartment with concrete ceilings between floors, it may be difficult indeed.
- . Do you object to the holes that must be drilled in walls, floors and ceilings to run wires?
- . What will comparable wired and wireless systems for your home cost?
- . What is the design of the home? A wired system may be more reliable in a multi-tiered dwelling or in one with several remote wings and additions. If you live in a bungalow, a wireless system may be ideal.
- . How maintenance-free do you want your system to be? Some people who object to changing transmitter batteries periodically may be better off with a wired system.
- . How unobtrusive a system do you want? If you object to the appearance of transmitters on your doors and windows, choose a wired system.
- . Do you plan to stay in your present home a long time? If not, a wireless system might be a better choice. (On the other hand, if you move, a good wired system can be an added selling point.)

[4] SENSORS

Sensors can be classified according to their application as perimeter and interior devices (a few--photoelectric beams and some sound discriminators, for example--can be used in either way). Perimeter sensors attach to walls, doors and windows. They trigger an alarm when a door or window is opened or forced, or when glass is broken. The following perimeter sensors are discussed in this report:

- . magnetic switches
- . window foil
- . frequency detectors
- . shock sensors
- . infrasonic sensors

Interior sensors (also called intrusion detectors or area alarms) protect the home's interior. They can be further divided according to their function as space protectors, weight detectors, sound discriminators and proximity detectors. The following interior sensors are discussed:

A/ Space Protectors

- photoelectric
- passive infrared
- ultrasonic
- microwave
- dual technology sensors

B/ Weight Detectors

- pressure mats

- stress sensors

C/ Sound Discriminators

D/ Proximity (Capacitance) Detectors

All interior devices are powered sensors (with the exception of pressure mats), requiring their own power source to operate (usually 12V DC). Many come in "stand-alone" or "slave" models. Stand-alone units are equipped with their own AC transformers for plugging into a wall outlet; "slaves" derive their power from the control panel. In a wired system, one pair of wires will carry the power to the sensor, another will carry the sensor's alarm signal to the panel via the protective circuit. Stand-alone units should be equipped with battery-backup in case of power failure. (Caution: most sensors are polarity-sensitive: connecting them incorrectly can damage the sensor and/or control panel).

Sensors are manufactured to operate as either normally open (N.O.) or normally closed (N.C.) devices. In a N.C. system, when all doors and windows on the same circuit are shut, the interconnected sensors form a closed circuit, presenting a certain value of voltage at the panel. This value must be present at the panel at all times when the system is armed; thus, if a component malfunctions or a wire is cut, the voltage drops and the system will alarm. The components of an N.C. system are thus "supervised" by the panel. In an N.O. system, there is zero voltage at the panel when all sensors are in their normal state (ie., not tripped). The circuit is closed only when an alarm condition exists. Thus there is no way to tell if there is no alarm because everything is secure or because the system is not functioning. In a N.O. system, cutting wires may or may not trigger an alarm. Most authorities advise that only N.C. systems be installed in residential settings. This

discussion assumes a normally closed system.

All sensors, whether perimeter or interior devices, should be designed to operate reliably despite fluctuations in line voltage and loss of power. Protection from radio-frequency interference (RFI) should also be built in. Sensors should be equipped with solid housings that protect the delicate internal circuitry and components from dust, moisture and (where applicable) insects.

Modern sensors are compact and designed to blend in with a home's decor. They come in several colour options. Most are surface mounted (a few have angled housings for mounting in the corner of a room). Most come with self-adhesive backing or a mounting bracket for easy installation. Optional flush mounting kits are also available. Any sensors designed for use outside the home should be equipped with tamper switches (sensors used inside the home do not generally require this protection).

Perimeter Sensors

Magnetic Switches

Also called reed switches (strictly speaking, the reed is the active component of the switch), magnetic switches are electromechanical devices used to detect an opened door or window. Each sensor has two parts: a switch and a magnet. One half is mounted on the door or window frame; the other is placed opposite it on the sash or door stile. The magnet keeps the thin metal reeds (contacts) of the sensor closed; when the door or window is opened, the magnet is removed and the switch springs open, causing an alarm.

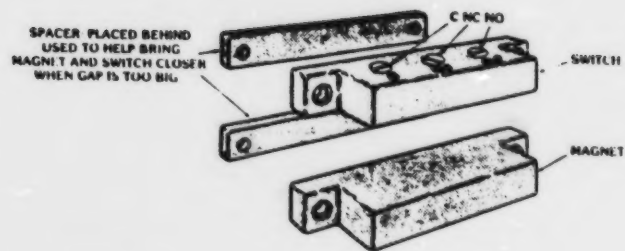


Fig. 3. Surface-mount magnetic contact switches.

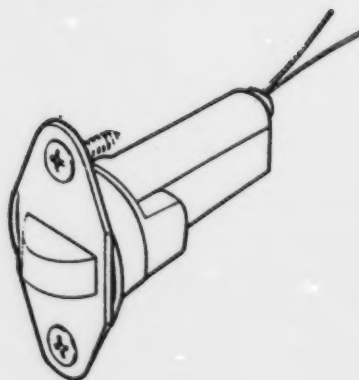


Fig. 4. Plunger-type magnetic contact.

Switches, especially those mounted on frequently used doors and windows, must be durable to withstand repeated use year after year. Better designs have sealed contacts. In unsealed units, moisture, humidity and airborne contaminants can corrode the contacts, causing the switch to malfunction. Even dust can be a problem.

Surface-mounted types are the most common, and are more easily installed. Miniature and micro-switches are available for use in places where space is at a premium. Recessed models are designed for use in fully concealed installations. Plunger and rollerball models combine the magnet and switch in the same housing, simplifying installation. Special switches are made for use on metal-framed doors and windows.

Magnetic switches are available in various gaps. Larger gaps are used to protect overhead and garage doors, loose-fitting or misaligned doors and windows, etc. Gaps of up to 5 cm (2") are possible. Installers have a choice of screw mounting or self-adhesive. Some switches come with a full, tamper-protected cover that hides the easy-access contacts and mounting screws.

Advantages

- . Most are simple and extremely reliable.

Disadvantages

- . Can be extremely difficult to conceal on some windows. Unconcealed units can be defeated by a knowledgeable intruder. (Some installers will avoid the problem by protecting window with interior traps.)
- . May require careful fitting and adjustment to operate properly. Use of spacers may be needed to achieve correct tolerances. Tolerances can change

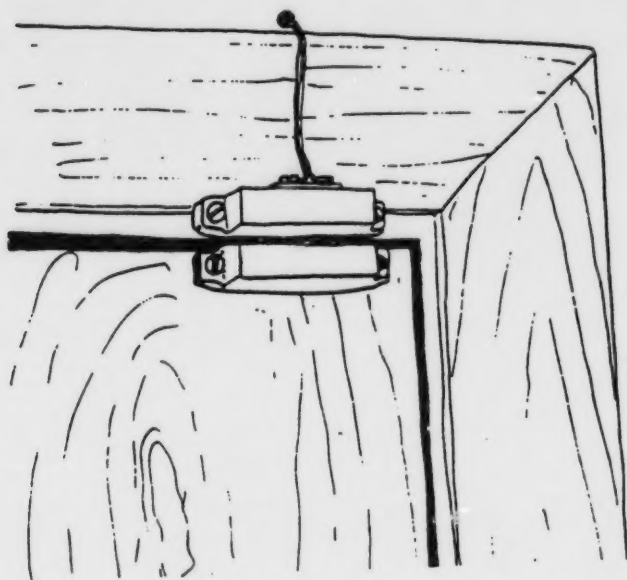


Fig. 5. Door-mounted magnetic contact.

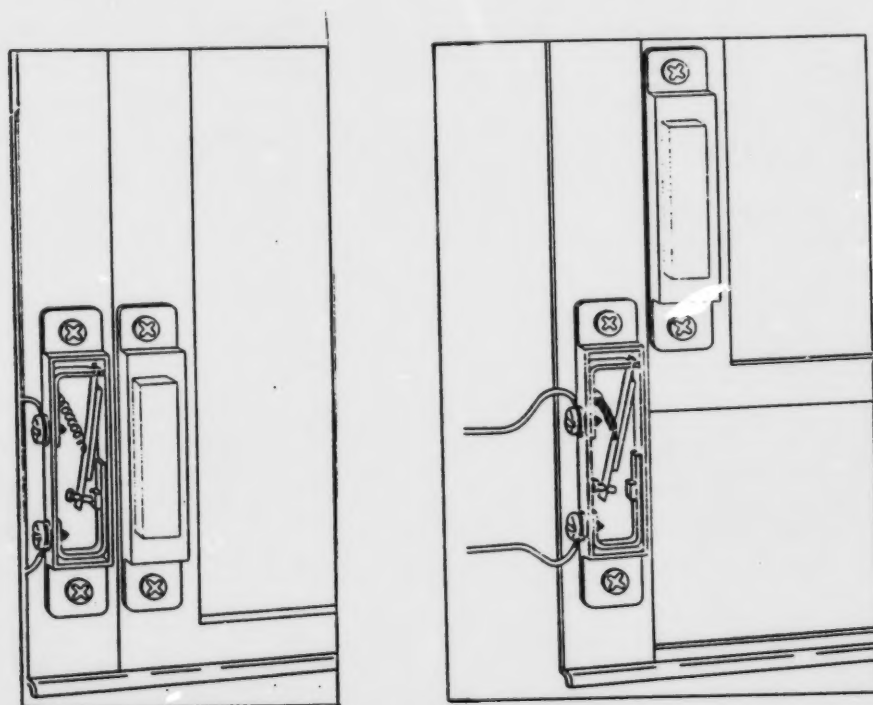


Fig. 6. Detail of magnetic contact mounted on double-hung window.

with time, requiring periodic re-adjustment of the sensor.

Window Foil

The sensor consists of strips of lead foil mounted on a window. The foil conducts a small current, forming a complete circuit. When the window is smashed, the foil breaks, opening the circuit and triggering an alarm. Window foil is an old and, by some accounts, obsolete technology.

Foil blocks (terminal strips) are used to attach the protective circuit wires to the foil. Plastic plug-and-socket ("pull-apart") connectors allow wires to be disconnected so that a window can be opened for ventilation. "Take-off" connectors can also be used. One half of the connector is mounted on the sash, the other on the sill. When the window is closed, the two halves touch, completing the circuit and allowing current to flow to the foil.

Foil should be applied to at least 75% of a pane's perimeter and covered with foil-protector (a clear lacquer) after installation.

Limitations/Considerations

- . Generally used only in wired systems.

Advantages

- . Inexpensive.
- . When working properly, very difficult to defeat. (Caution: Some brands use a self-adhesive lead/tin strip that resists breakage and may hold the pieces of a shattered window together.)
- . Simple to use: the foil is either continuous and working, or it isn't.

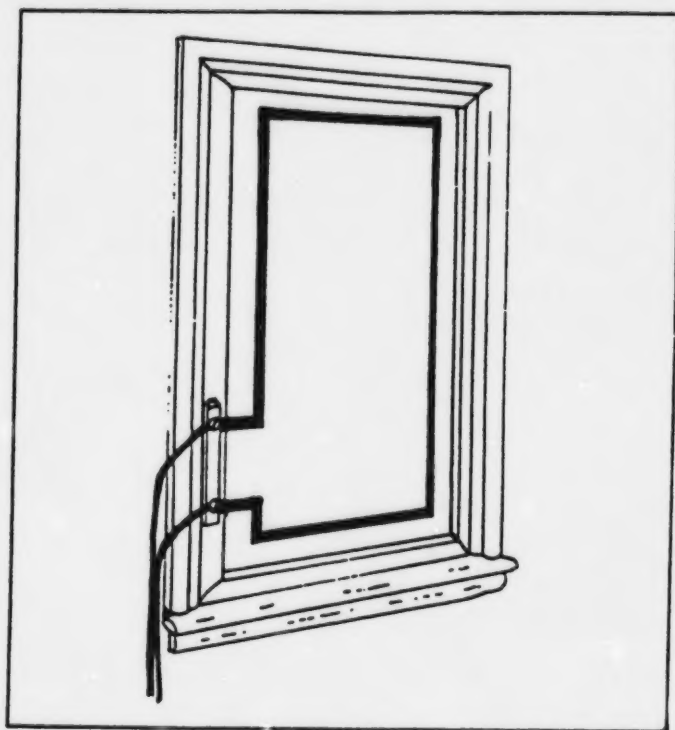


Fig. 7. Window foil.

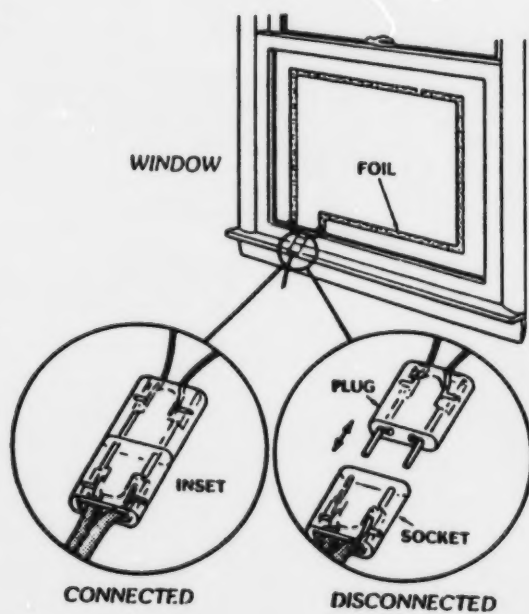


Fig. 8. Plug-and-socket foil connector.

- . Provides a visible deterrent (but warning decals do the same thing, more neatly).

Disadvantages

- . Unsightly (but may be suitable for basement windows, garage windows, outbuildings, etc.).
- . Easily damaged during normal activities (window washing, for example).
- . May need frequent repair & maintenance. When in poor repair, susceptible to false alarms. Some brands are susceptible to micro-breaks that are difficult to detect.
- . High labour costs for installation.
- . Difficult to apply properly (products are now available that simplify installation).
- . Deteriorates quickly: expands and contracts with weather. Connectors may be affected by condensation.

Frequency Detectors

Frequency detectors use a piezo-electric element to convert the frequencies generated by shattering glass into an electric signal. They are designed to be mounted directly on the glass using a self-adhesive backing.

Frequency detectors are generally used on easily accessible (main floor) windows and to protect glass panes in garages, sheds, solariums and door sidelights. They are especially effective on inoperable windows and skylights. They can be used on tilt-in windows and some doors if enough slack is provided in the wire lead. Glass in doors can be protected by using a



Fig. 9. Frequency detector.

flexible, coiled door cord. Typical coverage is a single pane up to about 1.2 m x 2.4 m (4' x 8') in size.

Limitations/Considerations

- . Very fast signal time; depending on the type of sensor and control panel used, may require a "pulse stretcher" to slow down the signal from the sensor enough that the panel can "read" it as an alarm signal.

Advantages

- . If installed properly, virtually impossible to defeat.
- . Being powerless, frequency detectors can't be short-circuited.
- . Unaffected by cold or magnetism.
- . Inexpensive and easy to install.

Disadvantages

- . Some are prone to false alarms caused by bells, jingling keys or vibrations caused by wind, traffic or machinery.
- . Do not report if window is opened but undamaged.
- . May be considered unsightly.
- . Self-adhesive on some units may deteriorate with age or from contact with moisture or sunlight, especially if carelessly installed.

Shock Sensors

Another type of glass protection is provided by shock sensors. These devices respond to the vibrations or flex of the glass created by an impact against it. The device usually consists of an adhesive-backed sensor and separate processor (some newer models do not require a processor). The processor, which is mounted in the main panel, analyzes signals received from the sensor and decides when a shock or vibration constitutes an attempted illegal entry. One processor can accommodate several (as many as 50) sensors. Some are designed for mounting on the glass; others can be frame-mounted. Better units can be individually adjusted for the type of service, mounting surface and background environmental conditions.

A few models combine both a frequency and shock detector in one unit to produce a more discriminating sensor.

Advantages

- . Often less prone to false alarms than frequency detectors.
- . Frame- or wall-mounted types can be used to protect adjacent windows or a

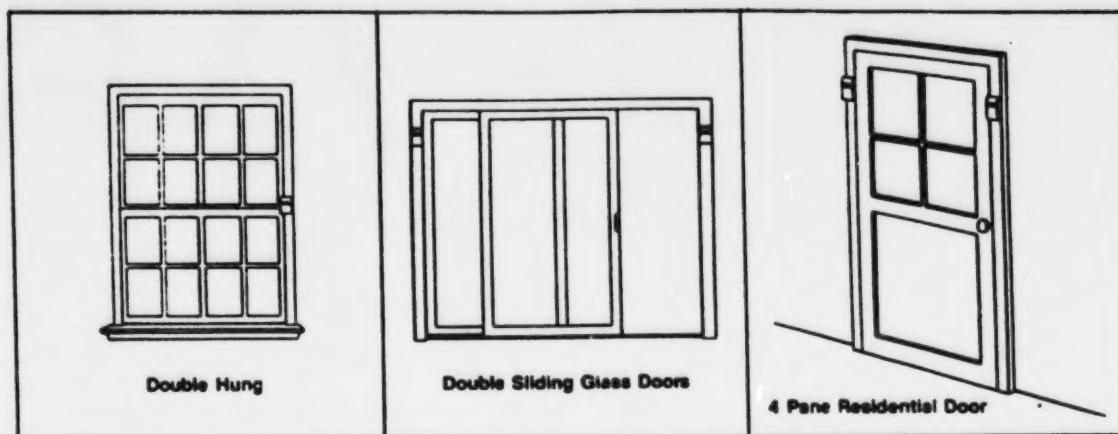


Fig. 9. Placement of shock sensors.

large window with multiple panes.

Disadvantages

- Less discriminating models may be triggered by rattling due to wind, machinery or traffic.

Infrasonic Sensors

These are passive devices that operate in the sub-audible region (.5 to 2 Hz) to detect minute changes in air pressure within a room when a door or window is opened. Infrasonic waves can pass through walls and furniture, allowing a single sensor to protect a very large area (up to 465 m² (5000 square feet)). They are extremely sensitive and can be used safely only in very stable environments. Not widely used in residential systems.

Interior Sensors

Photoelectric Detectors

These sensors emit a narrow, invisible (infrared) beam of light. An alarm is triggered when the beam is interrupted by an intruder. They are available in bounceback (transceiver) models and as two-unit models: in the former, the emitter and receiver are built into the same housing, and the beam is reflected by a mirror; in the latter, the emitter and receiver are two separate units that are mounted across from each other. Transceiver models are more common in residential applications, as they require less wiring.

Early versions used visible light, which could be seen and easily avoided or foiled by shining a flashlight into the photodetector. Newer models using frequency-modulated infrared light are much more reliable and difficult to circumvent. Emitters and receivers can be disguised as electrical outlets to increase their effectiveness. Photoelectrics are generally used as a kind of trip wire to protect single openings (eg. interior doorways), but occasionally find innovative applications (to protect a series of skylights, for example, or a long hallway with many doors opening onto it). Mirrors can be used to create a crisscross pattern to protect larger interior spaces.

Vertical alignment of the receiver with the emitter is critical for effective operation. Better units are equipped with a receiver LED to help position it correctly.

Limitations/Considerations

- Typical effective range is 23 m (75 feet).
- Should be mounted on stable surfaces only, not on frames or walls subject

to vibration or movement.

- . Should not be mounted facing windows exposed to direct sunlight.

Advantages

- . Can be mounted high enough to allow pets to pass underneath.

Disadvantages

- . Not produced in volume for residential use; may therefore be very expensive.
- . Easiest to detect and defeat of the interior sensors.
- . Of the interior sensors, protect the smallest volume of space.
- . May be difficult to align properly. Misaligned units can cause false alarms.

Passive Infrared Sensors

More passive infrared sensors (called PIRs in the industry) are manufactured and sold than any other single type of sensor (according to one source, 70% of all sensors sold are PIRs). PIRs are relatively inexpensive, use little current, are compact and provide wide-angle coverage, making them a favourite of installers and homeowners.

Like photoelectric, microwave and ultrasonic devices, PIRs are powered sensors; the term "passive" refers to the fact that, unlike the other three, PIRs do not emit any energy of their own. Instead, they convert the energy of the infrared radiation emitted by objects in their environment into electrical signals. (All objects that radiate heat--and virtually all do--are sources of

infrared radiation.)

Although there is considerable variation in the way PIRs by different manufacturers work, there is some common ground. Most designs use mirrors and lenses to focus on a number of discrete target areas in the room. The PIR adjusts to the difference in the radiation level emitted by these target areas and the background radiation of the room. When this difference is upset, as when a human body passes between the targeted object and the sensor--itself becoming the new target--an alarm is triggered.

In effect, the PIR creates "beams" or "fingers" of protection, as opposed to the volumetric protection afforded by microwave and ultrasonic sensors. The area defined by the fingers--the protection zone--is generally fan-shaped, with the narrow end located at the sensor. By changing lenses, a long, narrow pattern can be created for use in long rooms or hallways, or a wide, fan-

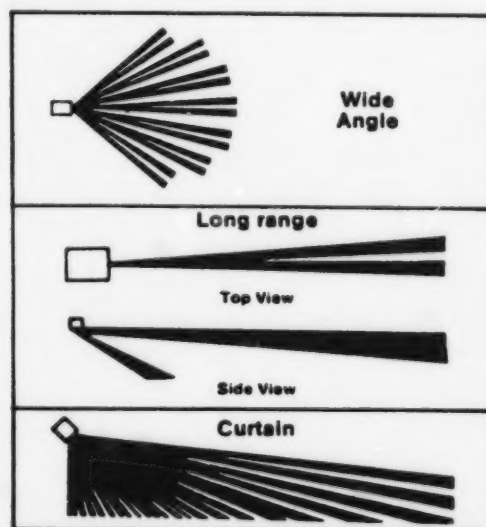


Fig. 10. PIR detection patterns.

shaped pattern for open areas. Generally, the more expensive the unit, the greater its range and sensitivity, and the larger the number of protection zones (typically 4 to 18).

PIRs are sensitive to changes in radiation levels. Any change in the established radiation level within a given protection zone, whether an increase or decrease, will trigger an alarm. Thus an alarm can be caused by a sudden change in the background radiation of a room (when a furnace shuts off, for example, and the temperature of the room drops) or by a change in the radiation emitted by a targeted surface (as when a picture falls off the wall, revealing the cooler wall surface behind it to the sensor). This principle, which is the foundation of the PIR's detecting ability, is also responsible for its false alarms. Alarms can be triggered by pets that walk into or out of a protection zone, a light bulb turning on or burning out, or a space heater switching on or off. Some units can be tripped by objects that are warmed rapidly by the surrounding air or incident sunlight, by a car's headlights flashing through a window as it turns up the driveway, or by light reflected from an outdoor pool. Since the amount of radiation reaching a sensor is inversely proportional to the distance of the source from it, a cat might pass undetected at a distance of five metres from the sensor, but could trigger it at a distance of two.

Manufacturers have devised various ways of overcoming (or at least limiting) the PIR's liabilities. Sensitivity can be adjusted to raise or lower the alarm threshold (Caution: sensitivity levels that were adequate for an overcast day in January, when they were set, may be too high on a sunny day in July). Some models respond only to disturbances of a minimum value over a set time interval, ignoring gradual changes in radiation levels. Various lens

options can be used to shape the protection zone to a particular environment, keeping individual fingers away from trouble spots such as hot air vents, radiators, air conditioners, wood stoves and light sources (including windows). Similarly, the field of view can be kept off the floor, creating a "pet alley" along which household pets and infants can pass without detection. This ability to limit and shape a PIR's zone of detection greatly reduces the incidence of false alarms.

Some PIRs respond to a change in a single detection finger; others ("dual element" detectors) look for a change in two adjacent fingers, registering the momentary imbalance created when a moving object is sensed a fraction of a second earlier in one finger than in the next. A simultaneous and equal change in any two adjacent fingers produces signals that cancel each other out, allowing the sensor to ignore global changes that affect the room as a whole. "Double pulse" units require that a radiating object move both into and out of the same "beam," or cross between two beams, before they will signal an alarm. In effect, these PIRs become motion detectors, ignoring changes in the radiation emitted by stationary objects. Still others use special internal circuitry that weeds out oscillatory motion (a curtain waving in the draft from a window or a swinging light bulb) but responds to a sustained or linear motion. Some use a "pulse count" system, in which successive disturbances within a preset interval have a cumulative effect on the sensor: the first two may be forgiven, while the third will push the sensor over its alarm threshold. A few models incorporate two or more of these methods in one annunciation logic. Little information, other than manufacturers' claims, exists on the relative effectiveness of these measures.

Modern PIRs are compact and attractively designed to blend in with a room's

decor. More expensive units will have better visible-light filters (visible light is a common cause of otherwise inexplicable false alarms with some PIRs).

PIRs are typically mounted 2 to 3 metres above the floor and aimed downward. Some are designed for ceiling mounting, which makes them even more difficult to approach without being detected and avoids blockage by furniture and partitions. Many wall-mounted units have a down-looking protection zone to guard against an intruder approaching the sensor along the wall on which it is mounted. All units should be provided with solid housings that protect the sensitive detector and mirrors, and keep out stray drafts, dust and moisture.

Limitations/Considerations

Infrared is a longer wavelength than visible light and may pass through some materials that are opaque to light and be blocked by others (glass, for example) that are transparent to visible light. When adjusting the sensor, care must be taken to ensure that the field of view is not blocked by furniture or partitions. Most sensors are equipped with a walk-test LED which allows the zone of protection to be defined.

The sensitivity of all PIRs decreases as the ambient temperature of the room rises. This is one reason why manufacturers recommend the units be adjusted so that each "finger" or detection zone terminates at the floor or other cool, stable surface (floors are normally cooler than walls and generally remain at a constant temperature). Also, the range will increase somewhat as temperature drops, making the detector sensitive to changes outside the protected area. Both sensitivity and range should be checked in different seasons and after making major changes to a room.

A PIR's detecting ability is greatest when the unit is located in such a way that an intruder must walk across the field of view (as opposed to moving toward or away from the sensor). Effective range decreases as angle of view increases; thus, deeper penetration into a long room can be achieved by sacrificing width of coverage. In hallways, a PIR is best used to protect against intrusion from the sides, through adjoining doorways.

Despite design features to prevent triggering by natural temperature changes, units should not be aimed at heat sources or windows, or be exposed to direct sunlight or direct blasts of hot or cold air. Keep moving objects and objects that can be moved by air turbulence (drapes, mobiles, suspended lamps, leafy plants) out of the sensor's field of view. Mount PIRs only on stable, vibration-free surfaces.

Despite the best precautions and design characteristics, unusual circumstances (or combinations of circumstances) can trigger false alarms. It is difficult to predict in advance what conditions will pass the sensor's alarm threshold. Actual testing with a particular unit in a given setting is the best policy.

Advantages

- . Infrared energy is blocked by most building materials, including glass. This reduces the possibility of radiation from outside the protected area infiltrating the room and causing false alarms (in rare cases, infrared energy can be reflected by smooth metal surfaces into a protected area).
- . Being passive, multiple units can't interfere with one another ("crosstalk"), so they can be used in arrays, to overlap coverage or protect each other.

- . Consume little power, making them ideal for wireless operation.
- . Ability to control and select the protection pattern reduces likelihood of false alarms.
- . Easy to install and maintain.
- . Reliable when properly installed and adjusted.
- . Difficult (but not impossible) to defeat.

Disadvantages

- . Depending on the model and manufacturer, may be triggered by car headlights, a flashlight, space heater,¹ light bulb, sunlight shining through a window or reflecting off glass or other polished surface, incident light heating objects in a room, curtains fluttering in a breeze, pets and vibrations caused by heavy traffic or machinery. A few can be tripped by radio frequency interference, which can be amplified by the sensor's internal circuitry to look like an alarm signal.
- . Solid objects can "block" the sensor, creating unprotected space.

Ultrasonic Motion Detectors

Ultrasonics were the first of the high-tech sensors. An active sensor, an ultrasonic emits high-pitched inaudible (20 to 50 kHz) sound waves, which are reflected back to it by the room and its contents. An object entering the protected space causes a shift in the frequency of the returning signal

¹ This can occur even if detection "fingers are aimed away from the heater; sudden currents of hot air produced by the heater may move into a sensor's field of view. If the sensor is overly sensitive, they may trigger an alarm.

(called the Doppler effect), which triggers an alarm.

Most modern units are transceivers (transmitter and receiver in the same housing). Better units have range and sensitivity adjustments and swiveling transducers, which allow the detection zone to be aimed to avoid probable sources of false alarms. On models with fixed heads, some directional control can be achieved by the use of deflectors placed over the transmitter.

On some units, a feature called "balanced signal processing" allows the sensor to ignore oscillatory motion (a curtain waving in a breeze). Other components filter out random sources of ultrasonic noise (the sound of steam under pressure, bells, phones, sirens, squeaky machinery and other alarms). Time delay circuits allow the sensor to tolerate air turbulence and other disturbances for up to 5 or 10 seconds before initiating an alarm. These provisions have made the newer units much less prone to false alarms than older models.

Better units are equipped with a separate walk-test LED for setting the range, and a background disturbance indicator which warns when a disturbance nears the unit's alarm threshold.

Limitations/Considerations

Ultrasonics typically provide volumetric (three-dimensional) protection to an area roughly 6 m x 9 m (20 x 30 feet).² Larger areas require multiple sensors. These must be carefully adjusted to operate on the same frequency to prevent one unit from triggering another.

An ultrasonic's range can be significantly reduced in a room with many soft

² This is under ideal conditions; in practice, better performance and fewer false alarms may be achieved at lower sensitivity settings. This is generally true of all powered sensors.

surfaces (heavy drapery, carpeting, stuffed furniture), which will absorb rather than reflect the sound waves. For some units, range will increase by as much as 1 metre at night when air turbulence is at a minimum. Initial adjustment should allow for this expanded range when the system is armed. Range may also be affected by temperature and humidity. A unit installed in hot, humid weather should be readjusted on a cold, dry day.

Large solid objects can effectively block the waves, creating pockets of unprotected space. The problem can usually be overcome by carefully planning the location of sensors and perhaps rearranging the room. Special units designed for ceiling mounting are also available.

Sound waves are normally contained by walls, doors and windows, but may reach through an open door if the signal is strong enough, allowing a disturbance outside the room to trigger an alarm. Ultrasonics work best in situations where an intruder would be forced to walk directly toward or away from the sensor. They are particularly effective in hallways and stairwells.

Like all powered sensors, ultrasonics should be mounted only on stable, vibration-free surfaces. Do not mount where the sensor will be subject to direct blasts of hot or cold air. Aim and limit the protection zone as much as possible to avoid sources of air turbulence (heaters, ducts, vents, open windows, air conditioners, loose-fitting exterior windows and doors). Keep moving objects such as fans, signs, curtains and pets out of the zone of protection.

Advantages

- Well-designed units that are properly installed provide a high level of detection and freedom from false alarms.

- . Very difficult to foil.

Disadvantages

- . Some models can be triggered by loud noises, slamming doors, keys jingling, phones ringing, doorbells, hissing steam from a kettle, a dropped glass, other alarms, the squeal of brakes, squeaky machinery, etc. Often sensitive to drafts.
- . Some units may interfere with other devices, such as remote-controlled televisions.

Microwave Detectors

Like ultrasonic detectors, these devices emit high-frequency sound waves (in the 10 GHz range) to detect the movement of solid objects in the protected space. Sound waves at this frequency can readily penetrate walls, requiring careful adjustment of the sensor to avoid extending the protection zone into an unwanted area. Although the coverage pattern is nonadjustable, range and sensitivity can be limited.³ Better units have separate LEDs that are an invaluable aid in making these adjustments.

Like ultrasonics, microwave detectors are typically mounted 2 to 2.5 metres (6 to 8 feet) from the floor and aimed downward.

Because of their expense and the difficulty of adjusting them, microwave detectors are rarely used by themselves in residential installations.

³ In theory, at least. In practice, it may be very difficult to establish suitable levels. A unit may be adjusted to ignore people moving about in the next room but be tripped by a truck passing in the street. The reason is that the truck's greater mass reflects more of the sensor's radiant energy.

Limitations/Considerations

Waves may be channeled from one area to another by heating ducts ("ducting"): avoid pointing the sensor directly at duct openings. Can be reflected by metallic or polished surfaces (including mirrors, water in bottles, foil-backed insulation in walls) to create unexpected patterns of protection.

Typical range is 9 x 9 or 9 x 15 metres (30 x 30 or 30 x 50 feet) in a tear-shaped pattern, with the sensor located at the narrow end of the pattern. Range and ability to penetrate non-metallic objects will vary somewhat with temperature and humidity. Should be mounted only on stable, vibration-free surfaces.

Advantages

- . Unlike ultrasonics and PIRs, microwave sensors are not usually blocked by solid objects. The penetrating ability of microwaves can be used to advantage: a single unit can be used to scan several rooms or be concealed behind a wall or above a suspended ceiling.
- . If properly installed and adjusted, these sensors are extremely effective at detecting intrusion.

Disadvantages

- . Expensive.
- . Penetrating ability and reflectivity of microwaves may frustrate attempts to find suitable levels.
- . May be set off by police radar, if very close and in a direct line.

Dual Technology Sensors

Dual technology sensors are a recent development in the industry's search for ways to reduce false alarms. Dual-techs combine two sensors in the same unit--either ultrasonic and PIR, microwave and PIR or infrasonic and PIR. The logic circuit triggers an alarm only when an intruder is sensed by both systems simultaneously and within a preset interval. In this way, the theory goes, the inherent weaknesses of the individual technologies are cancelled out, greatly reducing the number of false alarms.

Some units are equipped with a switch for normal or "high security" operation. In the latter mode, an alarm will be sounded when either component registers a disturbance.

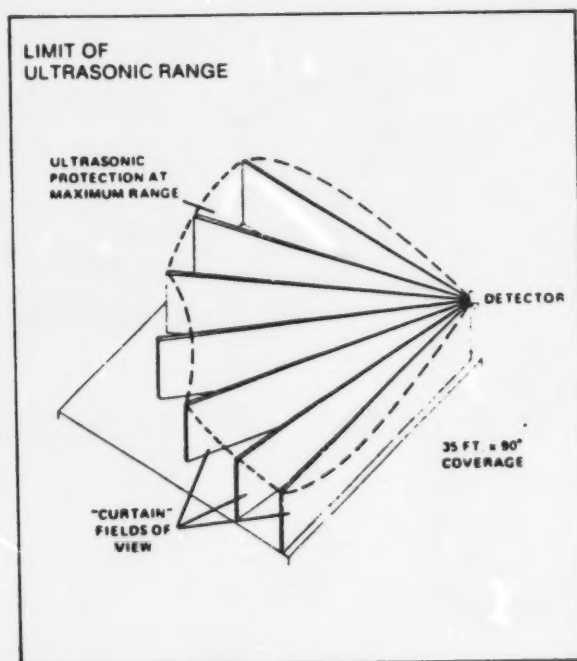


Fig. 11. Overlapping detection zones of a dual-technology (PIR/ultrasonic) sensor.

Because of their added cost, installers often reserve these devices for particularly harsh or unfriendly environments (factories, warehouses, garage bays, etc).

Limitations/Considerations

The range of both sensing devices should be adjustable, so that the zones of protection can be made to coincide as closely as possible. When the zone of one half the sensor extends beyond that of the other, it may be permanently tripped by an environmental disturbance. The sensor would not sound an alarm, but it would effectively be operating as a single-technology sensor.

Combining two technologies in the same housing has other drawbacks. Ultrasonic and microwave sensors are best located where an intruder will move toward or away from the sensor, but this is not the optimum situation for PIRs. If mounted incorrectly, one side of the sensor or the other may be at a permanent disadvantage.⁴

Advantages

- . Fewer false alarms.

Disadvantages

- . More expensive (up to twice the price of single technology sensors).

⁴ Better results might be achieved by using two single-technology sensors (a PIR and microwave, say) on adjacent walls, at right angles to each other, and leaving it up to the panel's logic circuitry to determine when an alarm condition exists. This arrangement would allow both sensors to work at peak efficiency and still verify each other. It is unclear whether any systems use this principle.

Pressure Mats

Pressure mats are used under a rug or carpet to trigger an alarm when stepped on. Like panic buttons, they are normally open devices--the circuit is closed when the parallel metallic strips in the mat are closed by the intruder's weight. Mats can be made more or less sensitive by applying layers of electrical tape directly over top of individual switch strips (for more sensitivity) or on either side of the strips (for less sensitivity).⁵

Mats come in sealed, pre-sized outdoor versions for use wherever there is a possibility of moisture, and in unsealed continuous rolls (1 metre wide) that can be cut to length for indoor use. Sealed versions should be used in breezeways between the house and garage, in porches, and under outdoor carpeting. They should also be used indoors under non-permanent carpeting or wherever they might be damaged by heavy use.

Some people install mats under window sills and carpets in cottages, leaving the sensor activated throughout the off-season.

Considerations/Limitations

- Low temperatures may reduce flexibility of the metal strips somewhat, reducing sensitivity.
- Bending the mat may damage it by putting a permanent kink or short in the metal contact strips, resulting in frequent false alarms.

⁵ "Pet-proof mats that require a minimum of 40 kg (90 pounds) to trigger an alarm are available.

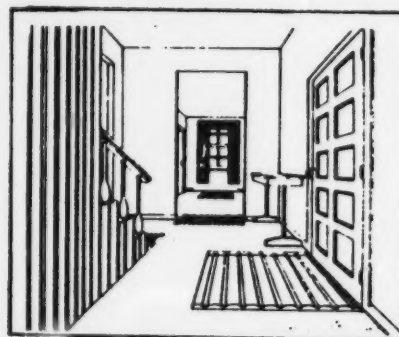
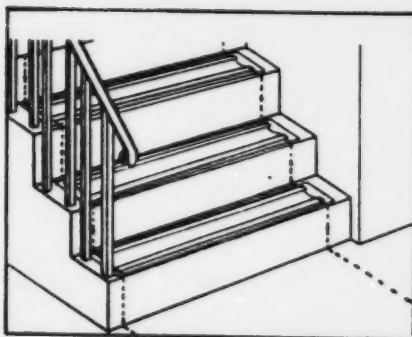
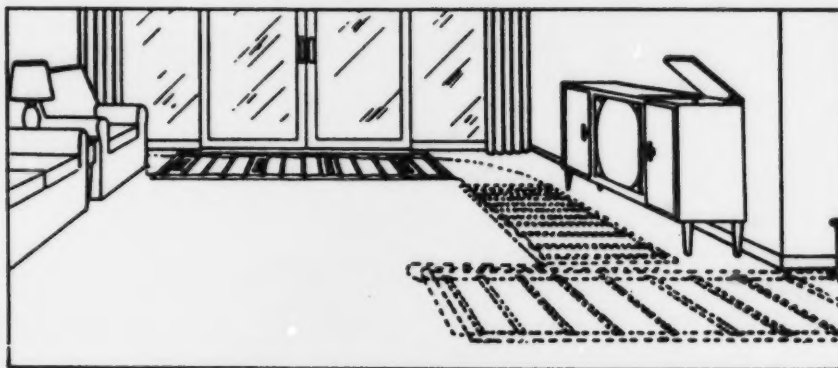


Fig. 12. Placement of pressure mats.

Advantages

- . Inexpensive and easy to install.
- . If properly located, can effectively do the job of more expensive sensors.

Stress Detectors

Like many shock sensors, stress detectors come in two parts--a remote sensing unit and an analyzer. Mounted on the underside of floor joists, the sensors are triggered by the stress imparted by an intruder's weight. The analyzer can be programmed to ignore natural changes caused by expansion or contraction of materials, settling foundations or rapid structural strain release. Most units have a sensitivity adjustment and a walk-test LED. Typically effective for a 1.5-metre (4-foot) radius around the sensor, they provide an effective way to create traps at entrances, stairway landings or hallways.

Stress detectors are a recent development and are not yet widely used. Their high cost and the difficulty of installing them makes their future uncertain.

Considerations/Limitations

- . Operate on 6V DC; therefore require their own primary and standby power supply.

Advantages

- . If properly installed, provide almost fault-free protection that is invisible and extremely difficult to defeat.

Disadvantages

- . Very expensive.
- . Extremely sensitive and delicate--must be handled with great care.
- . Difficult and time-consuming to install.

Sound Discriminators

A sound discriminator is essentially a microphone equipped with circuitry that is designed to discriminate between normal background noises and the sounds a burglar might make when breaking into a residence--shattering glass, splintering wood, the scrape of metal tools, etc.

Quality can vary enormously from one unit to another. Inexpensive models operate on a very wide bandwidth and are prone to false alarms. Better units are more discriminating, have separate adjustments for frequency and volume of the protected space, and are equipped with a LED to help set levels.

A few models are highly directional and are designed to provide perimeter protection for windows. Mounted on a ceiling and aimed at a window (or array of windows), they can do the job of several frequency or shock detectors.

Limitations/Considerations

Typical range is 5 metres (16 feet), but will vary depending on local acoustic conditions. These sensors provide effective protection if used wisely and appropriately. Do not mount near doorbells, telephones, air conditioners or similar devices that may generate interference noise. Suitable for non-living areas of the home: eg., garages, breezeways, basements, porches, solariums.

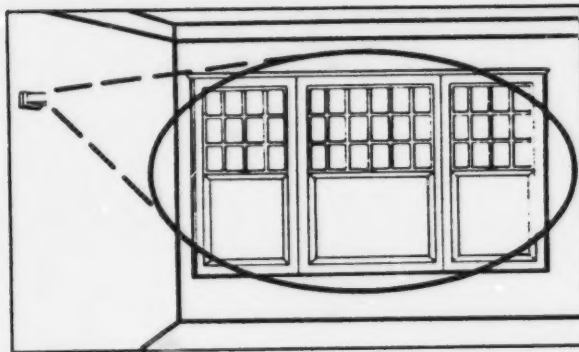


Fig. 13. Directional wall-mounted sound discriminator can protect several windows.

Advantages

- . A single unit can be used to protect multiple windows.

Disadvantages

- . Inexpensive models are prone to false alarms. Can be set off by door knockers, doorbells, telephones, and other everyday noises.
- . Unlike shock and frequency detectors, most models can be used only when the protected area is unoccupied.

Capacitance (Proximity) Detectors

These devices are used to protect a single object. They surround the object

with a weak electrical field, which is attenuated or distorted when the object is approached, causing an alarm.

Inexpensive battery-operated units are sometimes mounted on door handles in motels and hotels to give a traveller an added measure of security. More expensive units are used in commercial settings (to protect wall safes and filing cabinets, for example). Not widely used in residential installations.

Limitations/Considerations

- . Can only be used on metallic objects.

Advantages

- . Compact and inexpensive.



Fig. 14. Capacitance door alarm.

Disadvantages

- . Prone to false alarms. Some models are sensitive to humidity.
- . Once armed, nothing within the electrical field can be moved without causing an alarm.

Other Devices

Trip wires are sometimes used to protect basement windows, gable vents, trap doors and other uncommon access points. These devices use a thin nylon cord that is easily broken and virtually invisible. An alarm will sound when the cord is broken or dislodged from between the metal contacts of the wall- or frame-mounted anchor.

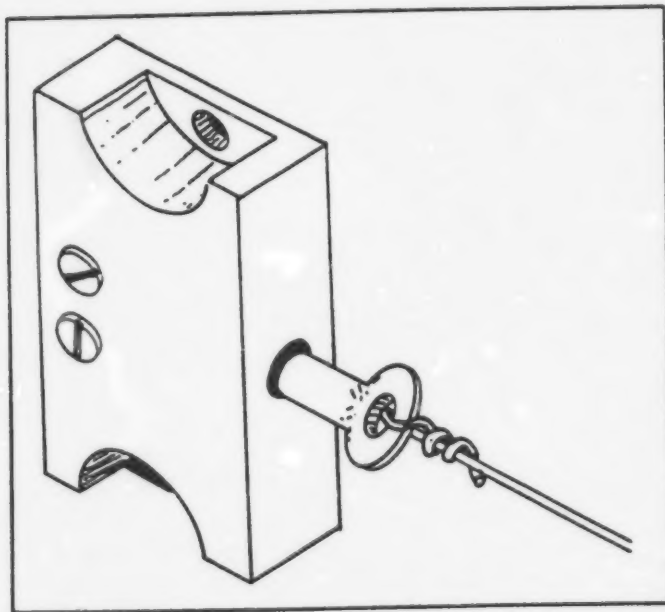


Fig. 15. Trip wire will trigger alarm when pin is pulled from its anchor.

Special window screens laced with a thin conducting wire are also available. These devices provide good window protection even when the window is open for ventilation. Screens are usually made-to-measure to fit a particular opening.

Panels

Control panels are the "brains" of an alarm system. Electronic circuits process (ie. interpret) signals sent by individual sensors and take appropriate action (sound a siren or horn, initiate a local and/or remote alarm, trigger a dialing device, etc.). Modern control panels are in effect central processing units, similar to those found in home computers. Most operate on 12V DC using a step-down transformer.

The latest generation of panels is modular in design, providing great flexibility in tailoring a system to the needs (and/or whims) and lifestyle of a particular customer. Basic capabilities can be extended simply by adding the appropriate modules (circuit boards).¹ Every good control panel should include these features:

- A choice of instant and delay circuits. Sensors connected to an instant circuit (all windows and seldom-used doors, for example) will trigger an alarm as soon as they are disturbed; those on a delay circuit will initiate a countdown toward alarm. If the countdown is not aborted by the homeowner either at the panel or from a remote control station, the alarm will sound. This provision allows a system to be disarmed from inside the house after

¹ Modular controls also permit a system to be easily upgraded or repaired.

entering the home (entry delay) or before leaving (exit delay).² The delay feature is often combined with an audible prealarm warning and flashing light as an additional reminder to the homeowner to turn the system off after entering.

- . Acceptance of both normally open (N.O.) and normally closed (N.C.) sensors. Although most sensors used in residential installations are N.C., a few (pressure mats, panic buttons, keyswitches) are N.O. devices.
- . End-of-line resistor (EOL). This is an anti-tamper measure that was until recently used only in high-security installations, but has now become available on residential systems (one indication that burglars are becoming more knowledgeable and resourceful). EOL-equipped panels are designed to "see" a certain minimum resistance across the protective circuit at all times to know that all is well. The protective circuit, which links all the sensors, becomes a "supervised loop." This prevents an intruder from bypassing a sensor by short circuiting it out of the system.
- . Fail-safe arming. Systems equipped with this feature will not arm if a door or window in the protective circuit is ajar. This eliminates one of the most frequent causes of false alarms.
- . Adjustable timed alarm cycle and automatic reset. A valuable tool for avoiding irate neighbours in the event the alarm is tripped by accident

² ULC recommends a 1 minute maximum for exit delay and 15 seconds maximum for an entry delay (45 seconds maximum if a keyswitch or pushbutton keypad are used for disarming).

during the owner's absence.

- . Status indicator lights and alarm memory. Status indicator lights are LEDs mounted on the panel and remote control stations that show at a glance whether the system (or parts of it) is armed or disarmed. Alarm memory works in the same way. Flashing LEDs are used to warn the homeowner that the system has been tripped during his/her absence (more elaborate systems will show which zone or sensor was tripped). This is more than a convenience feature: mounted on a remote control in the garage, for example, a flashing alarm memory light could prevent a homeowner from entering his/her house, in which the intruder could still be lurking. This feature is especially useful for systems not monitored by a security company. Also very useful for troubleshooting the system for persistent sources of false alarms.
- . 24-hour panic circuit that allows use of an emergency panic button. Panic buttons can be mounted in strategic locations throughout the home, as well as incorporated into control panels and remote control keypads. Some come as pendants or hand-held wireless units for pocket or purse. They allow the homeowner to activate the system on command, whether the system is armed or not. They are also useful for summoning help in a medical emergency. Panic buttons should be kept out of reach of children and curious visitors. Some come with fail-safe protection (requiring two buttons to be depressed simultaneously, for example). (Note: Most authorities caution against activating an audible alarm when in direct confrontation with an intruder.)

- . Rechargeable standby batteries capable of supplying from 4 to 6 hours of backup power in the event of a power failure or deliberate interruption of primary power to the panel. How much backup power is enough depends on the size of the system, which will determine the rate of power use.³ Batteries are generally gel-cell or lead-acid types. Gel-cell batteries charge quickly but may be damaged if allowed to run down too low. They must also be mounted upright to avoid leakage of the corrosive electrolyte. Lead-acid batteries are less prone to damage by deep discharge and are leak-proof. Better panels have a built-in charging system to insure the standby battery is always fully charged. Those that use non-rechargeable dry cell batteries should include a low-battery warning. Rechargeable batteries may last 6 to 8 years with regular recharging; dry cell batteries may need to be replaced every few months.

With increasing miniaturization and programming sophistication, designers are now able to offer a dizzying array of optional "convenience" features that would satisfy even the most gadget-hungry homeowner. Some of the more useful options include:

- . Automatic timers for turning lights and select appliances on and off to give a home that "lived in" look that discourages most opportunistic thieves.
- . Zoning capability. This feature allows the entire system to be subdivided

³ ULC recommends a minimum of 4 hours of backup power. At the end of 4 hours, the backup source should have enough reserve power to operate an audible alarm for 4 minutes.

into separate zones. The panel can be set to disarm select zones while keeping the rest of the system armed. Thus, the perimeter system might be armed while interior sensors are disarmed when the family is at home, providing "at-home protection." In more elaborate systems, a malfunctioning sensor can be temporarily excluded ("shunted") from the protective circuit. The balance of the system continues to provide protection until a repair technician can be called. Typical wired panels keep track of about 8 zones; wireless controls using digitized transmissions can manage 15 or 20, and a few offer as many as 80, one for

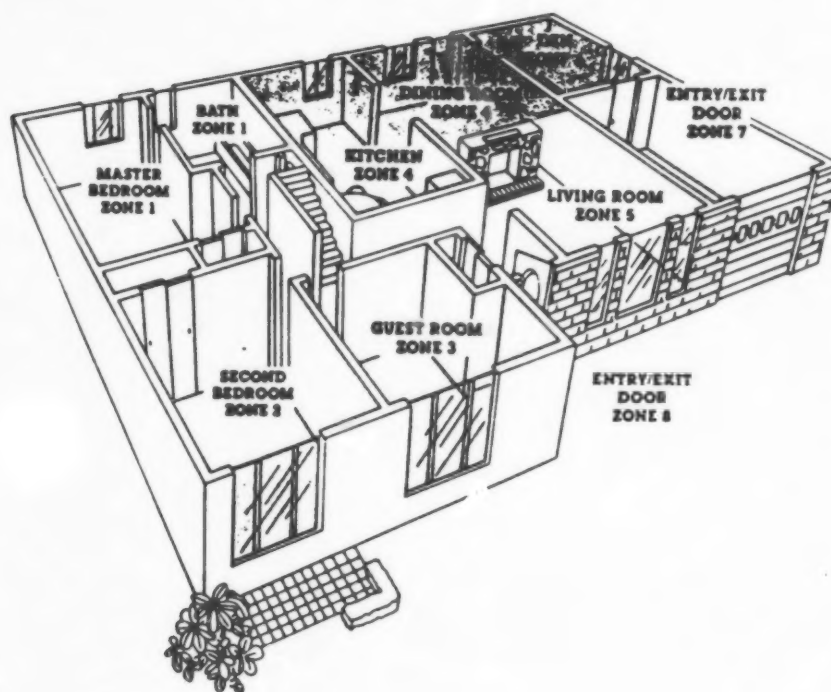


Fig. 16. Advanced panels will monitor several zones independently of each other.

each sensor in the system. (In some systems, the number of zones can be increased by adding a device called a "zone expander.")

- . Test buttons that allow all parts of the system to be tested without initiating an alarm. Especially important in unsupervised systems.
- . Separate codes for initiating an audible panic alarm, an inaudible panic alarm that is transmitted direct to the monitoring station, and a duress alarm (used to secretly signal the monitoring station that the subscriber may be under duress).
- . Code control. This feature allows secondary and "babysitter" access codes to be established and deleted. A secondary code might be entrusted to a house guest or maid, giving them partial control of the system. When the guest or maid leaves, the secondary code can be deleted, without all resident users having to learn a new code. "Babysitter codes" are designed for one-time-only use, after which they are automatically erased from the system's memory.

These features can be activated from a pushbutton pad built into the panel or from a remote control station, fixed or portable. Several manufacturers now offer complete control of the alarm system via any pushbutton phone located on or off the premises.

In order for the latest microprocessor-based panels to function, they must be properly programmed. The number and types of sensors used; their configuration (instant or delay); shunting capabilities; the details of the

supervisory functions; what is to be interpreted as an alarm signal and what is to be ignored; how the panel is to react when an alarm signal is received--all this information, and more, must be "burned into" the panel's PROM (Programmable Read-Only Memory). Some controls are programmed at the factory, others must be programmed at the time of installation. Programming is done at the panel using a portable programmer provided by the alarm company. A few very recent models allow the PROM to be programmed directly from the panel's keypad or by remote control from the monitoring station. Individual sensors must also be coded and identified to the panel using a series of dip switches.

Programming ability allows a system to be tailored to a particular user's needs. However, there can be problems. Codes can be entered incorrectly or, once entered, forgotten by the owner. The PROM's memory can be scrambled by lightning-induced power surges. In some models, programmed information may be wiped from the panel's memory by a power blackout. Some panels have built in batteries or other safeguards that will hold programmed information in memory until power is restored ("non-volatile" PROMs); others have no such protection and may need to be reprogrammed. All programmable systems should be carefully verified before use. Buyers should ask their alarm dealer about the measures built into the panel to guard against loss of programmed information.

All electrical equipment can be damaged by lightning. Neither the structure nor the alarm hardware need sustain a direct hit to be damaged: damage can result from a near miss that creates high induced currents in the home's electrical system, metal ductwork, conduits or other metal raceway. Control panels, which contain extremely sensitive electronics and circuit boards, must be protected from lightning-caused power surges. Manufacturers have developed a variety of ways to limit the damage that can be done by

lightning. The methods used are too technical to be discussed here⁴; it is enough to note that some form of lightning protection is essential. Purchasers should be aware of the problem and ask about the protective measures that have been designed into a control panel to guard against lightning damage.

One measure that can be taken in the case of all panels is proper grounding. Direct earth grounding using a heavy-gauge copper wire (16 gauge minimum) and a copper rod (or copper-clad steel) is best. The wire should be run to ground along the most direct path possible, avoiding loops and turns. Connection to an underground metal water pipe is also effective, provided that there is good electrical contact between the grounding wire and the metal pipe. The practice of grounding the panel through the home's electrical system is less effective. For the highest level of protection, all externally mounted noise makers and their metal enclosures should be similarly grounded.

Panels may also be affected by transients or "spikes"--sudden and unpredictable surges or fluctuations in line voltage. Spikes are sometimes created when power is returned to the electrical system after an outage or when a heavy inductive motor is started (floor polisher, table saw, etc.). In some panels, a transient voltage can scramble the microprocessor, producing erratic behavior of the alarm system and possibly necessitating a complete reprogramming. Better panels are equipped with some form of protection to

⁴ Protective measures include spark gaps, gas discharge tubes, non-linear resistors, "self-healing" components that temporarily break down in the presence of destructive currents, lightning-resistant circuitboard design, and capacitive/inductive delay networks that slow a surge down enough that other protective devices can handle them effectively.

prevent this from happening.⁵

Many panels allow smoke detectors, water-level alarms, heat sensors, etc. to be wired into the system. If this is done, the panel should be designed so that the sound produced for an intrusion alarm is different from that produced for the other types of alarms.

Panels should be fully protected against tampering and be adequately protected from moisture, fire and dust. They should be mounted in a concealed location, preferably where access is protected by a sensor. Basements and main-floor clothes closets are the customary locations.

Some words of caution: All security is imperfect, and each system is a product of a set of compromises. Some offer certain features at the expense of others, more or less security at the expense of (or in favour of) easier access, convenience, lower cost or ease of installation. Perhaps the best advice that can be given a prospective buyer is this: decide on how much security you need and then buy the system that will do the job, but no more. Beware of high-pressure salesmen who try to sell you a more elaborate alarm system than you may really need. Multi-feature panels sound good in theory and look impressive in sales brochures, but many people who install them later become intimidated by their complexity and end up using only a small portion of their capabilities. Homeowners must decide for themselves which features are important additions to security and which are frivolous and needlessly complicating.

Some features may even undermine security. Remote programming capability, for example, may be nice to have in the event that you forget your system's

⁵ Some panels use the backup battery as a type of capacitor to filter out transients.

codes or if your children give out the code to friends. But in the hands of inexperienced monitoring station operators or an unscrupulous alarm company, such capability could prove a security hazard. The onus is on the alarm owner to be aware of what functions the monitoring station is able to carry out by remote control and to negotiate carefully to limit these functions.

Remote Controls

Installed in strategic locations throughout the home (the bedroom and wall adjacent to the main entrance are common locations), a remote control allows an owner to arm/disarm the system (or parts of it) without going to the main control panel. Remote controls, or "remotes," are either mechanical keyswitches or digital pushbutton keypads. Possession of the right key or authorized user code allows the owner to identify himself/herself to the panel and prevents unauthorized access to the system.

Keyswitches are less expensive but inherently more vulnerable to tampering. If you are buying a remote keyswitch, ask carefully about the built-in tamper features. Techniques for protecting the all-important remote control are varied and imaginative. A qualified security professional can be very helpful in this area.

The other weakness of keyswitch remotes, of course, is that it is always possible to lose or misplace the key.

Pushbutton remotes arm or disarm the system when the button is pushed or a prearranged code is punched into a keypad. These devices provide greater security but can be very expensive (some cost as much as the control panel), and there is always the danger of forgetting the code. Pushbutton remotes can

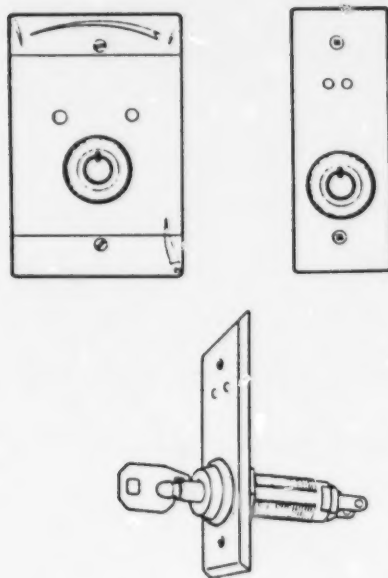


Fig. 17. Keyswitch remote controls.

be extremely sophisticated, offering full or partial control of system functions. Most are equipped with automatic lockout, which shuts the unit down if the wrong code is repeatedly entered (to prevent an intruder from trying to guess the code).

The quality of pushbutton remotes varies greatly. Inexpensive models are not recommended, as they are unreliable and vulnerable to tampering. An entire alarm system can be compromised by a single poorly designed remote control. Generally, units designed with a separate decoder (logic board, which is mounted in the main panel and which interprets the digital data from the keypad) provide greater security. (Caution: not all pushbutton remotes will work with all panels.) Wireless hand-held remote controls are also available. These can be simple panic buttons or fully programmable keypads

that can duplicate most of the functions of the wired stationary remotes. Wireless remotes are battery-operated transmitters that send coded radio signals to a strategically located receiver (the receiver may be placed next to, but not inside, the main panel). They provide unparalleled convenience, allowing the homeowner to turn the alarm system on or off from anywhere within the home, the driveway or the adjacent grounds.

Wireless remotes have several drawbacks. Some suffer from "dead spots": the signal may not be received by the receiver from certain locations in the home. Another is the need to remember the codes. Perhaps a more serious drawback is the risk that the unit will malfunction and lock the owner out of the home (all such devices, of course, should be equipped with a low-battery warning). Some units can also be jammed by a neighbour's garage-door opener.

Local or Remote?

Detecting an intruder is just part of what an alarm system does. Making sure someone knows about it is the other part. Reporting systems can be either local or remote, or both. A local alarm alerts only the home's occupants and immediate neighbours. A remote system sends a signal to a third party, usually an alarm monitoring station.

A local alarm can be sounded by a bell, siren or horn. Remember that the local alarm has three aims: to alert the homeowner, scare off the intruder and summon help. To do this it must be loud. Underwriters Laboratories of Canada recommends a minimum of 87 dB when measured at a distance of 3 metres (10 feet) from the source. Check local bylaws, which may restrict the loudness of such equipment.

External reporting devices can be complemented with an internal annunciator. These are particularly useful if the external device is highly directional or if the home is large and the external warning may not be heard from all parts of the residence or grounds. Specially designed sirens are available for use inside the home, but a simple 12 V DC piezoelectric buzzer (a small, low-voltage, solid-state buzzer) may also be adequate. For an added measure of security, the house and yard lights can be wired to turn on when the alarm sounds. Strobe lights may also be added to give impressive visual effects. In a crowded neighbourhood, strobes and wired-in house lights can help police locate the source of the alarm.

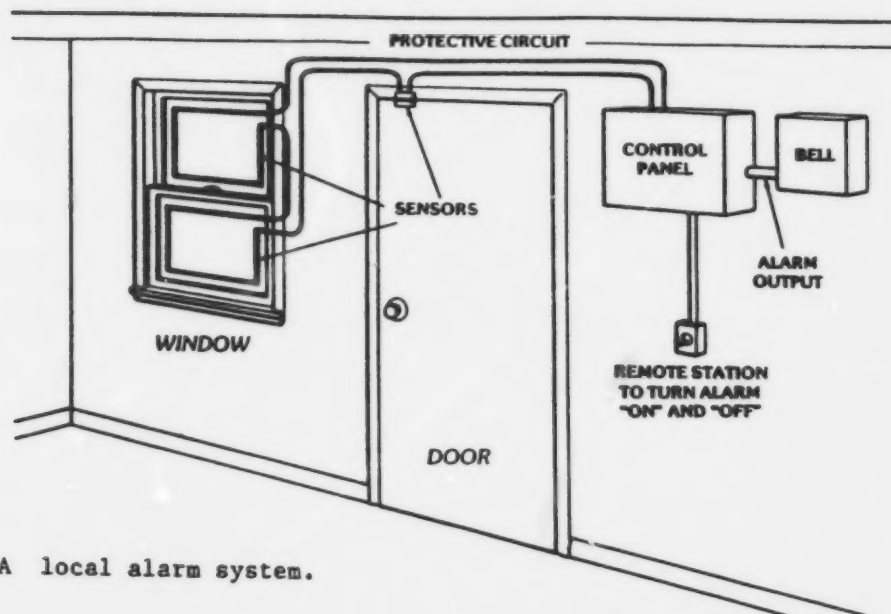


Fig. 18. A local alarm system.

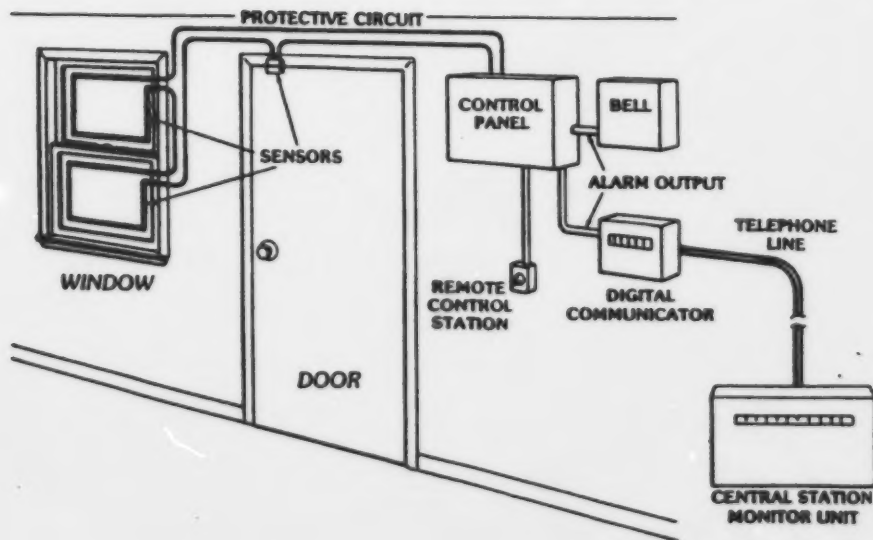


Fig. 19. A central station alarm.

A local alarm is obviously less expensive and relatively easy to install, but its usefulness is limited. In rural or suburban areas where neighbours are distant from one another, an intruder may decide to ignore the alarm, assuming that it will not be heard. An especially steely nerved intruder may decide that he/she can collect the valuables and escape before help arrives. Local alarms can be masked or disabled by clever intruders, allowing them to go about their business undisturbed.

Bell or Siren?

Bells are cheaper and provide the traditional ringing sound associated with burglar alarms. A bell is less directional than a siren, but its range may be limited by trees, shrubs etc. Use a bell in a populated area where range is not as critical, and a siren in a suburban or rural area where distance between neighbours is greater.

Most sirens have two-channel capability: they can emit two different kinds of sounds--a rise-and-fall and a steady tone. Use the former for the burglar alarm system, the latter for fire and other emergencies. If the nearest neighbour is more than 300 metres away, choose a unit that emits a long rise-and-fall sound, which is heard better at a distance than the shorter yelp. As mentioned, sirens are highly directional, with the volume falling off rapidly as you move away from the line of travel. Keep this in mind when positioning the unit.

Sirens come in separate driver-and-speaker models and as self-contained units (driver is built into the speaker). Because sirens use little current, a single driver can power as many as eight separate speakers. Bells, on the

other hand, consume current; installing more than one in the same system is not advisable. The separate driver/speaker types are generally more powerful.

Whether you choose a bell or siren, it must be protected from tampering. Noisemakers should be concealed and mounted out of reach in solid, tamper-proof enclosures. Enclosures should be equipped with tamper switches front and back--that is, to protect against the lid being pried open and against the entire enclosure being pried from the mounting surface. External enclosures should be resistant to rain and ice buildup.

Mount external noisemakers high on a side wall, aimed in the direction from which help is most likely to come. A good place is behind the louvers of an attic gable vent. (Caution: the louvers may muffle the sound somewhat; test



Fig. 20. Installing an alarm bell.

after mounting to be sure levels are adequate.) Protect all wires from tampering by running in steel conduit. This is especially important if the device cannot be mounted well out of reach. Remember that a burglar who gains access to the garage may have the use of your ladder and other tools. Another device is to use electrical cable to make the bell or siren wire look like part of the home's electrical system. Few intruders will risk cutting it with metal pliers to find out whether it is really a 120 V line.

Interior sirens can be mounted on a high wall or ceiling. Mounting inside a heating duct, where the noise will be amplified, may be very effective. Do not mount near the control panel, to avoid giving away its location.

Tape Dialers

A good addition to a local alarm is a tape dialer. The device is connected to the telephone line and may be programmed to automatically dial one or more numbers when an alarm is sounded. Some models will continue dialing if a busy signal is received until a call is answered. When a connection is made, the machine plays back a prerecorded message, giving the nature of the emergency and the home's location.

These devices have their limitations. They are useless, of course, if the phone is dead. Inexpensive models may "dump" their message even when no line connection has been established. And there is no guarantee that the outgoing message has not been received by an answering machine.

In some areas in the U.S. tape diallers can be used to place a call to the local police station; most forces, however, discourage this practice. Police recommend that the machines be programmed to call a responsible individual--a

neighbour or relative--who could then determine if the emergency is real before summoning authorities.

Central Station Alarms

In a remote reporting system, the alarm signal is communicated to a remote location, usually the monitoring station of an alarm company. The station's staff take appropriate action, either dispatching a security guard or repair technician, calling to verify that the alarm is real, and/or notifying the police, depending on the nature of the alarm and the arrangements made in advance with the homeowner. Monitoring stations charge a fee for their service--typically \$20-\$30 per month, depending on what is monitored and the type of signal transmission used. Some stations offer a complete home monitoring service, warning of furnace or freezer failure, a burst water pipe, overflowing sump, and so on.

In most residential installations, a device called a digital communicator is used to transmit the alarm signal from the home to the central station via the dial telephone network. When an alarm condition occurs, the communicator seizes the telephone line to which it is connected to send a coded signal to the monitoring station. A receiver at the station translates the coded message into a computer readout, giving the address of the home, the type of alarm and, sometimes, information on which sensor has been tripped.¹

¹ Bell Canada now requires that a special security jack be installed in every home using a digital communicator. Care must be taken in wiring the communicator to the jack. If the jack is incorrectly wired to the system, the communicator will be unable to seize the telephone line if the line is in use. The connection can be tested for correct wiring by taking the phone off the hook and deliberately tripping the alarm system.

Dialers and digital communicators must meet technical specifications

The communicator may be an integral part of the control panel or an add-on (a modular circuit board that can be snapped into the panel or removed without affecting the system's overall functioning). Some companies sell the communicator outright; others prefer to lease it to the subscriber for the duration of the monitoring contract. The latter arrangement allows the company to remove the communicator in the event of a contract default, thus avoiding annoying calls from non-subscribers. Care must be taken when choosing a communicator as an add-on component, as some may not be compatible with a given station's receiving equipment.

Some form of digital communicator is in use in 80% of homes equipped with central station monitoring. Although the system provides an inexpensive communication link between the subscriber and the monitoring station, it has one great weakness: the alarm signal cannot be sent if the telephone wires are cut. A communications link between the monitoring station and subscriber is established only when an alarm is signalled. There is thus no way for the monitoring station to tell whether no signal is being received because a subscriber's home is secure or because the wires have been cut or equipment has malfunctioned. Most alarm owners seem content to live with this weakness. They reason--quite accurately--that most burglars will not go to the trouble of cutting a phone line. In many places, the lines are buried and cannot be cut.

People who want line security have several options open to them. For an additional fee, some stations will periodically poll all subscribers to verify that the phone link is intact. Some advanced systems can be programmed to call in to the station at prearranged intervals. If a system fails to report

established by the Department of Communications.

on schedule, the station may assume that an alarm condition exists.² Some companies will sell and install a line monitoring device ("line sniffer") as an optional extra. These devices continuously monitor the line and will signal a local alarm if the line is cut. Another solution involves incorporating a backup radio transmitter into the home's alarm system. In the event of a cut telephone line, the transmitter would automatically send a radio message to the monitoring station. Such a system would be expensive and bulky. For these reasons radio frequency backups are not widely used.³

Another alternative is to lease a "dedicated" phone line from Bell Canada. A dedicated line can be continuously monitored, so that any tampering with it is immediately detected. However, because of the shortage of such lines and the expense involved in leasing them, dedicated lines are seldom used for residential applications.

An alternative to telephone communication between the home and the central station is afforded by the cable TV network. Cable is an extremely wide bandwidth medium and can accommodate an enormous volume of signals. Because of this, it affords the potential for low-cost, two-way communication between home and central station along a continuously monitored line. However, to do this, a two-way cable must be used, rather than the one-way cable that many

² I say "may" here, as not all firms will treat a missed check-in as an alarm; some may dispatch an employee to investigate the next day.

³ It would also have to be DOC approved.

A few of the newest wireless systems use a form of transmitter backup called the "buddy system." If a disconnected phone line prevents one system from transmitting its alarm signal, it will automatically contact a nearby "buddy" system, which will place the call for it. Both "buddies" must be made by the same manufacturer.

Long-range radio supervision may be more widely available in the near future. A major American manufacturer/distributor (Ademco) has developed a radio frequency (RF) system, and an American-made RF communications link is being readied for sale in Canada, pending DOC approval.

companies have already installed. To convert to two-way cable may be prohibitively expensive for many firms. Cable monitoring is available in a number of locations in the U.S., but at present in only one or two Canadian cities. Monitoring costs are comparable to that of normal unsupervised monitoring via a telephone link and digital communicator.

A recent development in telephony provides still another option. Called derived channel, the technique sends a continuous stream of low-frequency signals over the telephone line. The signal is well below the audible range and does not interfere with normal conversation. Any tampering with the line can be immediately detected at the station. The technology was developed in the U.S. and was first applied in Canada. It is currently available only to subscribers in Winnipeg, Brandon and Selkirk, Manitoba, where it is known as the FAST system.



[7] THE COST OF PROTECTION

The cost of installing an electronic alarm system is extremely difficult to predict. Prices will vary, depending on:

- . where you live
- . the design of your home (the interiors of some open-concept designs can sometimes be protected with a single sensor)
- . the level of security desired
- . whether you install the system yourself or have a professional do it for you
- . the security company you choose
- . the type and configuration of the system you buy (wired/wireless; supervised/unsupervised)
- . ease of installation
- . how effectively sensors are utilized
- . the options and convenience features you desire
- . the quality of the equipment used
- . whether you choose a local or central station alarm
- . etc., etc., etc.

Battery-operated portable alarms used to protect a single door or window are available from consumer electronics stores or by mail order for \$30-\$50. More expensive models come with a built-in keypad for arm/disarm control and for setting entry/exit delays.

For \$100-\$200 consumers can purchase stand-alone, plug-in alarms that

include a sensor (usually an ultrasonic or PIR device) and built-in noisemaker. The limitations and liabilities of such equipment have already been discussed.

Budget component systems sell for \$200-\$600. Most of these "package" systems are wireless. The cheapest models include one or two pairs of magnetic contacts, a control unit and internal (or external horn). Additional sensors (including an interior space protector--again, usually PIR), panic button and remote keypad may be offered as optional extras at additional cost.

Professionally installed wired alarm systems start at about \$1200; "average" installations run \$1500-\$1800. A frequently used estimate places the cost of a wired alarm system at about 1%-1.5% of a home's market value. Top-end systems may cost \$10 000 and up, depending on the size of the home and the level of protection desired. In fact, the cost of protection is limited only by what the owner is willing to pay. On average, labour costs account for 20-30% of a system's purchase price.

The price of a wired systems has a great deal to do with ease or difficulty of installation. A system costing \$2000 to install in one home could cost as much as \$3000 to install in another.

Basic wired systems include contacts on all main-floor entries, a control panel and remote keypad, panic button, single interior sensor (usually PIR), smoke detector and internal/external noisemaker. Window protection is usually extra.

Basic wireless systems with minimal supervisory ability can be installed for around \$1200. More elaborate systems with full supervision and zoning features will cost up to \$5000.

Service contracts for professionally installed wired systems may cost \$300-

\$400 per year. Monitoring costs range between \$200-\$350 per year. Central station alarms using a digital communicator include a one-time installation cost of about \$50 for the Bell Canada jack. FAST system users in Manitoba pay a line fee, ranging between \$5 and \$25 per month, depending on the number of services being monitored (burglary, fire, water pressure, panic etc.).

Typical costs for alarm components are given below.¹

window foil (per window)	\$20-\$40
magnetic contact switches	\$20-\$65
frequency detector	\$30-\$250
shock sensor	
sensors (each)	\$30-\$50
analyzer	\$100
infrasonic sensor	\$150
photoelectric sensor	\$700
passive infrared sensor	\$50-\$200
ultrasonic sensor	\$150-\$260
microwave sensor	\$400-\$600
dual technology sensor	\$200-\$700
pressure mats	
indoor, 32" wide, per foot	\$6-\$10
outdoor, 2' x 3'	\$100
sound discriminator	\$75-\$120

¹ Figures shown are retail prices for installed equipment. Markups of 200% to 300% over wholesale are not uncommon in the industry.

stress (seismic) sensors		
sensors (each)		\$50-\$60
analyzer		\$220
control panel		\$100-\$700
keypad		\$60-\$300
panic button		\$20-\$50
horn/siren		\$50-\$250

Some firms lease rather than sell their alarm systems. Leased systems go for about \$30-\$45 per month and may include full servicing for the duration of the lease. The cost of periodically updating the system as new equipment becomes available is usually shared between the client and the alarm company.

[8] CHOOSING AN ALARM COMPANY

Security companies appear and disappear with astonishing frequency. One survey showed that of the 140 alarm companies listed in the Yellow Pages of a large metropolitan area, 30% were actually out of business. In signing a contract with an alarm company for the installation and monitoring of your alarm system, you are entering into a long-term business relationship. Choosing the right partner in this relationship is well worth the effort involved. Remember too that, next to yourself, the people who will know the most about your security system--its layout and limitations--will be the people you choose to install it. Here are some things homeowners can do to be sure they choose the right company:

- . Call your local office of the Better Business Bureau to see if any complaints have been lodged against the firm.

- . Ask friends, neighbours, relatives and co-workers who might have an alarm system about the company that installed it. Ask about the company's ability to install the equipment right the first time, the neatness and efficiency of the installation, the knowledgeability of its agents, its promptness in responding to service calls, and so on. Alternatively, ask the company you are considering for the job for referrals (other clients the company has served) and call them. Although most companies will be unwilling to give a referral, citing the security and privacy of their clients, it will not hurt to ask.

- . Ask how long the company has been in business. The answer will not be conclusive, by any means, as many new firms are responsible and trustworthy, while the best and most reasonably-priced service is not always provided by the most established companies. Nevertheless, years-in-the-business is at least one measure of a company's standing and viability.

- . Ask if the firm is a member of CANASA. Although many reputable alarm companies are not CANASA members,¹ a firm's membership in this organization is one indication of its credibility. CANASA members have a least 5 years' experience in the alarm business, must comply with the Association's code of ethics, and must carry a minimum of \$1 million liability insurance against claims arising from faulty installation or failure to respond to an alarm signal. Equally important, homeowners have additional recourse through the Association in the event of a disagreement with a member firm. The Association will investigate complaints lodged against a member and, where warranted, take action against it.

- . Ask if the company installs ULC-approved equipment. There is a great deal of good equipment available that is not ULC approved, but ULC approval does give homeowners a degree of protection.²

¹ Only 20% of Canada's estimated 1500-2000 alarm companies are CANASA members.

² Only a small proportion (perhaps 10%) of equipment available for residential use is ULC tested. The ULC tests for fire and electrical safety, durability, audibility of reporting devices and resistance of the equipment to a wide range of environmental conditions, including temperature, humidity and voltage fluctuations. For a listing of ULC-approved alarm equipment write to: Underwriters' Laboratories of Canada, 7 Crouse Road, Scarborough, Ontario, M1R 3A9.

- . Ask whether the firm will back up its product lines, regardless of whether they become obsolete, are discontinued or are manufactured by firms that go out of business.
 - . Ask about the warranty. Warranties should assure satisfactory operation of the system and replacement of all defective parts. A one-year term is average.
 - . If you will be buying a monitoring service, ask if the central station has a ULC rating. Depending on the rating, ULC-approved stations must have on-site monitoring staff around the clock every day of the year. They must keep accurate records of all alarm signals received (including details of the follow-up) and are subject to periodic inspection by ULC auditors. Although ULC standards apply only to stations involved in monitoring high-risk commercial installations (comparable standards for residential monitoring services have yet to be established), a ULC rating may offer a homeowner an added measure of security.
 - . Ask about the maintenance contract (if you want one). Ask about the cost and when service technicians will be available. Some companies offer full maintenance service at no additional cost for the duration of the monitoring contract. Hours of service vary: some are limited to normal business hours, others will dispatch a service technician at any hour of the day or night.
-

- . If installing a central station alarm, ask carefully about who will monitor the system, where the station is located, and the method of communication that will be used. Some firms sub-contract the monitoring function to another company, which may have no office in your area (this is not necessarily a disadvantage, but homeowners should ask about the response procedures that will be followed). Others have staff on-site only during normal office hours; after-hours service may be provided by on-call personnel.

- . Ask how the communication line is protected and what provisions will be made for detecting severed communication links or faulty transmitting equipment.

- . Question the company closely about how it will respond to an alarm signal and how soon a response can be expected. Some firms treat all alarms as real and notify the police immediately. Others may call the subscriber's home and/or neighbours to verify that the emergency is real. Still others have different response procedures, depending on the type of alarm received. Ask whether the company will charge a fee for responding to a false alarm and whether it offers a key service.³

- . Ask if the company has backup power to enable it to continue to monitor your home in the event of a major power blackout. For how long?

³ In the interest of avoiding liability, some firms will not offer a key service (in which a copy of the key to the subscriber's home is kept at the monitoring station to allow its agents to service the system and/or investigate alarm signals). Others will place the key with a security company.

- . You may wish to ask whether the company's installers and technicians are bonded, and about the training they receive.⁴

You can learn a lot about a company by paying a visit to its monitoring station. If the company is hesitant about allowing this or is evasive about answering your questions, take your business elsewhere.

Perhaps the best advice is to get price quotations and installation proposals from several firms before making a decision. Proposals should spell out exactly what equipment will be used in which locations, and the cost of all parts and labour. When comparing prices, be sure you are comparing apples with apples. Some firms can significantly undercut competitors by using inexpensive and unreliable components.

Before signing an agreement, be sure you have all details of the quotation, the warranty and service contract in writing. Be especially wary of any contract containing a universal disclaimer releasing the firm from all responsibility, regardless of what it does or does not do.

How to Recognize a Security Professional

Qualified security professionals are trained in the theory and design of alarm systems. They will know about and be able to advise the homeowner on the range of available options. Unless the person is an independent security consultant, of course, the options he/she presents will likely be limited to

⁴ Poorly trained alarm installers and technicians are a continuing liability for the industry. CANASA-sponsored certification courses for alarm installers are now offered by Seneca College (Toronto), Red River Community College (Winnipeg) and Vancouver Community College.

the equipment sold by his/her company.

Here's how to recognize a security professional:

- . In planning your system, a security professional will conduct a thorough security evaluation of your home. He/she will note the home's overall layout, the placement of bedrooms, location of main internal traffic arteries, the locations of doors and windows, and the type and location of valuables. He/she will point out weaknesses in your basic security (poor locks, hollow doors, vulnerable garages, overhanging trees, poor exterior lighting, etc.) and encourage you to attend to these areas before installing an alarm system.
- . He/she will ask about the tenants, and whether there are any children, elderly people and pets in the home.
- . She/he will ask about who will operate the system, and whether any cleaning people, maids and other staff will need access.
- . He/she will be aware of local bylaws and ordinances that pertain to electronic alarms, including those governing false alarms, and will advise the homeowner about them.
- . She/he will tailor the alarm system to the home's design and the owner's needs and lifestyle, keeping in mind the value of the property to be protected.

- . He/she will use the right sensor in the right place to provide maximum effective coverage and reduce the risk of false alarms.

- . When the installation is complete, she/he will take time to educate the homeowner in the system's proper operation, indicating clearly what the system can and can't do, and outlining the procedures and user habits to be followed for efficient, trouble-free operation of the system.



[] GLOSSARY

Access codes Security codes that must be entered into a keypad by an authorized user, allowing him/her to arm, disarm or reconfigure an alarm system.

Alarm memory Ability of some systems to report whether an alarm was initiated during the owner's absence.

Alarm threshold The maximum level of disturbance that a sensor will tolerate before triggering an alarm.

Backup power A battery installed in a control panel to supply the alarm system with power in the event of a power failure.

CANASA Canadian Alarm and Security Association

Central Station Alarm An alarm system designed to transmit alarm signals to a monitoring station, usually via telephone lines.

Contention Jamming of a wireless system's receiver by multiple signals.

Control panel The alarm system's main signal processing centre.

Controls Control panels, keyswitches, keypads and panic buttons.

Crosstalk The tendency of nearby ultrasonic sensors to interfere with one another, particularly if they are operating at nearly identical frequencies.

Dedicated line A telephone line used exclusively for monitoring an alarm system.

Delay circuit Control panel circuit with a built-in adjustable alarm delay. Sensors connected to a delay circuit will trigger an alarm only after the delay interval has elapsed.

Derived channel A method of ensuring the integrity of the telephone link between an alarm system and the monitoring station by transmitting a continuous stream of sub-audible signals along the line. Cutting the line interrupts the signals and triggers an alarm.

Digital communicator A device for automatically establishing a telephone communications link between an alarm system and a remote monitoring station when an alarm is sounded.

Dual technology sensor A sensor that combines two different methods of detecting an intruder in a single device.

End-of-line resistor (EOL) A fixed-value resistor wired into a protective circuit to warn of any attempt to short-circuit a sensor.

Entry delay A preset interval during which the alarm will not sound after a

sensor is tripped. An entry delay allows an alarm to be aborted by a homeowner after entering the home.

Exit delay An initial interval during which no alarm will sound after the system is armed. An exit delay allows a homeowner to leave the home after turning the system on, without triggering an alarm.

Frequency detector A sensor designed to respond to the high-frequency sound produced by shattering glass.

Hardwired system A wired alarm system.

Infrared radiation Electromagnetic energy with a wavelength between that of visible light and radio waves. Some infrared energy is radiated by all objects at a temperature above absolute zero.

Infrasonic sensor A sensors attuned to frequencies below that of audible sound.

Instant circuit Control panel circuit that has no delay feature. Sensors connected to an instant circuit will trigger an alarm the instant they are tripped.

Interior sensors Sensors designed to protect a home's interior spaces.

Keypads Pushbutton panel controls.

Keyswitch Key-operated arm/disarm switch.

LEDs Light-emitting diodes.

Local alarm An alarm system that triggers a local bell, horn or siren.

Magnetic contact switches Two-part sensors used to warn when a door or window is opened. One half contains a magnet, the other contains a pair of thin metal contacts.

Microwave detector An interior sensor that uses microwaves to detect motion.

Monitoring station An alarm or security company's facilities for monitoring subscriber's alarm systems.

Noisemaker A device for creating an audible alarm warning.

Normally closed (N.C.) Refers to sensors and circuits that offer an uninterrupted path to an electrical current when no alarm condition exists.

Normally open (N.O.) Refers to sensors and circuits that are open under normal (non-alarm) conditions, permitting no current to pass.

Panel An alarm control panel.

Panic button A pushbutton switch for immediately initiating an alarm, whether

the system is armed or not.

Passive sensors Sensors that do not emit energy. Includes passive infrared and infrasonic sensors, pressure mats and some frequency detectors.

Passive infrared sensor An interior sensor that responds to changes in infrared energy levels in its field of view.

Perimeter system The network of sensors used to protect a home's exterior doors and windows.

Photoelectric sensor A sensor that emits a continuous beam of light. The sensor triggers an alarm when the beam is interrupted by an intruder.

Powered sensors Sensors that require electrical power to operate.

Pressure mat A sensor designed for use under a carpet or rug to detect an intruder's weight.

PROM Programmable Read-Only Memory. The place where information is permanently stored in a control panel's processing circuits.

Protective circuit In a wired system, the continuous copper path along which alarm signals are transmitted from the sensors to the control panel.

Proximity (capacitance) detector A device that generates a weak electrical

field around a metallic object. Any attempt to disturb the object will alter the electrical field and trigger an alarm.

Radio frequency interference (RFI) Random radio-frequency signals that can interfere with an alarm system's receiving or control equipment.

Remote A remote control.

Remote control A device such as a keyswitch or pushbutton keypad that gives a user control of an alarm system without having to go to the control panel. Remote controls can be permanently mounted or portable.

Remote reporting system An alarm system that directs its alarm signals to a remote location, usually a central monitoring station.

Reporting system Those components of an alarm system designed to signal, through audible or visual means, that an alarm condition exists.

Sensor A device used to detect an intrusion or attempted intrusion by sensing changes in established environmental conditions (motion, sound levels, radiation levels, etc.).

Shock sensor A sensors that is designed to trigger an alarm when there is an impact against, or vibration within, the surface on which it is mounted.

Shunted sensor A sensor that is temporarily excluded from the protective

circuit of which it is a part.

Slaves Sensors that rely on power from the control panel to operate.

SMD Surface Mounted Devices. The term refers to a type of microelectronic circuit design that minimizes the effects of radio-frequency interference.

Sound Discriminator A sensors designed to detect sounds that might be created during an attempted break-in.

Stand-alone sensor A sensor that draws its power directly from the home's electrical system through a wall outlet.

Stress sensor A sensor designed to detect the stress imparted to floor joists by a person's weight.

Supervision The ability of an alarm system to monitor itself to detect and report equipment malfunctions.

Tamper switch A spring-loaded switch or other device used to detect any unauthorized tampering with an alarm component.

Tape dialer A device that automatically dials one or more phone numbers when an alarm condition occurs, and plays back a prerecorded message.

Transceiver A radio-frequency transmitter and receiver combined in the same

housing. In the case of a photoelectric sensor, a design that combines the emitter and receiver in the same housing.

Transients Intermittent fluctuations in line voltage. Also called "spikes."

Traps Interior areas protected by a sensor.

Trip wires Fine, almost invisible wires stretched across an opening to warn of any attempt to pass through it.

ULC Underwriters' Laboratories of Canada.

Ultrasonic sensor A sensor that uses high-frequency sound waves to detect motion.

Walk-test LED A light on a sensor that turns on to indicate that the sensor has been tripped, even though the alarm system may be disarmed. LEDs are useful for making initial sensitivity and range adjustments after a sensor is installed.

Window foil Current-carrying lead foil taped to a window to warn when the window is broken.

Window screen A specially made wire-laced screen used in place of a normal window screen to warn of attempted access through it.

Wired system An alarm system in which signals are transmitted from the sensors to the control panel via a continuous run of copper wire.

Wireless system An alarm system that uses miniature radio transmitters to send the alarm signal from the sensors to the control panel.

Zone expander A device used to increase the number of separate zones supervised by the control panel.

Zoning capability Ability of some systems to separate the sensors into groups or "zones," and to monitor each group independently of the others.